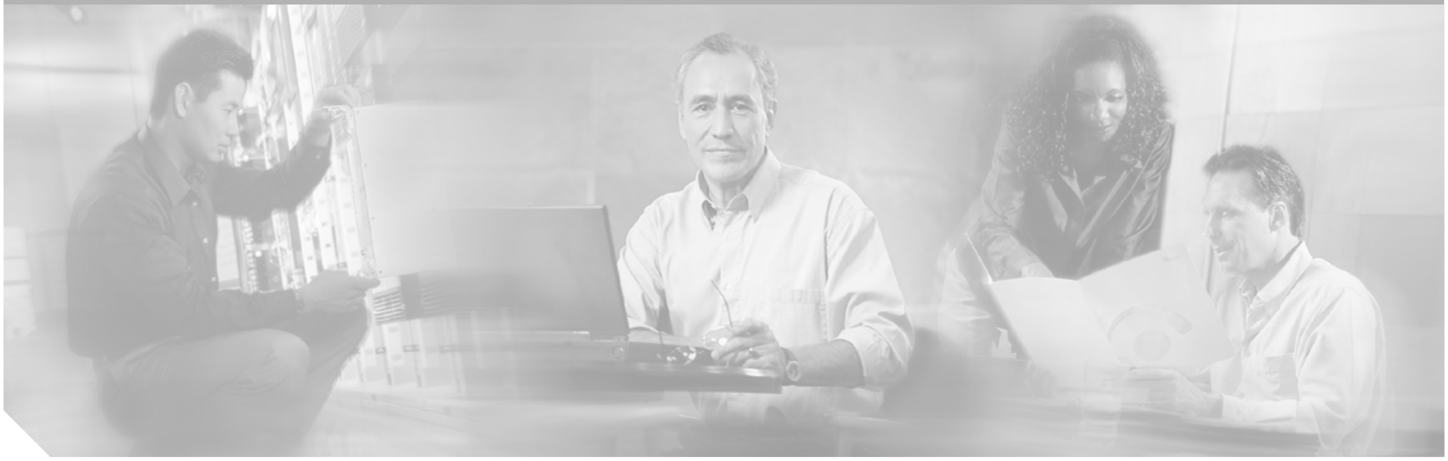


Cisco Access Registrar 3.5 Concepts and Reference Guide

July 2004

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Customer Order Number:
Text Part Number: OL-2683-02

Cisco Access Registrar 3.5 Concepts and Reference Guide

CONTENTS

About This Guide

This document provides information to help you understand RADIUS concepts and to help you develop a better understanding of the Cisco Access Registrar 3.0 server. This document contains the following chapters:

- Chapter 1, "Overview," overview of the RADIUS server, including connection steps, RADIUS message types, and using Cisco Access Registrar as a proxy server.
- Chapter 2, "Understanding Cisco Access Registrar," describes the Cisco Access Registrar object structure, and explains when Cisco Access Registrar references each of these objects during the processing of client requests.
- Chapter 3, "Cisco Access Registrar Scripts," describes the scripts provided with Cisco Access Registrar.
- Chapter 4, "Understanding Replication," describes Cisco Access Registrar's configuration replication features, functions, limitations and operation.
- Chapter 5, "Understanding SNMP," provides information about Cisco Access Registrar support for SNMP.
- Chapter 6, "Prepaid Billing Solution," describes the generic call flow between the three components required to support a prepaid billing solution using the RADIUS protocol: the AAA client, the Cisco Access Registrar 3.0 server, and a prepaid billing server.

This guide also contains a Glossary and an Index.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco Product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

Attn Document Resource Connection
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

http://www.cisco.com/register/

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

http://www.cisco.com/tac/caseopen

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

CHAPTER 1

Overview

The chapter provides an overview of the RADIUS server, including connection steps, RADIUS message types, and using Cisco Access Registrar as a proxy server.

Cisco Access Registrar is a RADIUS (Remote Authentication Dial-In User Service) server that allows multiple dial-in Network Access Server (NAS) devices to share a common authentication, authorization, and accounting database.

Cisco Access Registrar handles the following tasks:

- Authentication—determines the identity of users and whether they may be allowed to access the network
- Authorization—determines the level of network services available to authenticated users after they are connected
- Accounting—keeps track of each user's network activity
- Session and resource management—tracks user sessions and allocates dynamic resources

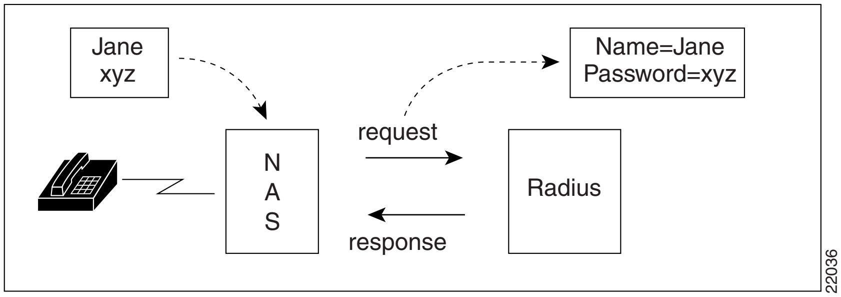
Using a RADIUS server allows you to better manage the access to your network, as it allows you to store all security information in a single, centralized database instead of distributing the information around the network in many different devices. You can make changes to that single database instead of making changes to every network access server in your network.

RADIUS Protocol

Cisco Access Registrar is based on a client/server model, which supports AAA (authentication, authorization, and accounting). The *client* is the Network Access Server (NAS) and the *server* is Cisco Access Registrar. The client passes user information on to the RADIUS server and acts on the response it receives. The *server*, on the other hand, is responsible for receiving user access requests, authenticating and authorizing users, and returning all of the necessary configuration information the client can then pass on to the user.

The protocol is a simple packet exchange in which the NAS sends a request packet to the Cisco Access Registrar with a name and a password. Cisco Access Registrar looks up the name and password to verify it is correct, determines for which dynamic resources the user is authorized, then returns an accept packet that contains configuration information for the user session (Figure 1-1).

Figure 1-1 Packet Exchange Between User, NAS, and RADIUS



Cisco Access Registrar can also reject the packet if it needs to deny network access to the user. Or, Cisco Access Registrar may issue a challenge that the NAS sends to the user, who then creates the proper response and returns it to the NAS, which forwards the challenge response to Cisco Access Registrar in a second request packet.

In order to ensure network security, the client and server use a *shared secret*, which is a string they both know, but which is never sent over the network. User passwords are also encrypted between the client and the server to protect the network from unauthorized access.

Steps to Connection

Three participants exist in this interaction: the user, the NAS, and the RADIUS server. The following steps describe the receipt of an access request through the sending of an access response.

Step 1 The user, at a remote location such as a branch office or at home, dials into the NAS, and supplies a name and password.

Step 2 The NAS picks up the call and begins negotiating the session.

a. The NAS receives the name and password.

b. The NAS formats this information into an Access-Request packet.

c. The NAS sends the packet on to the Cisco Access Registrar server.

Step 3 The Cisco Access Registrar server determines what hardware sent the request (NAS) and parses the packet.

d. It sets up the Request dictionary based on the packet information.

e. It runs any incoming scripts, which are user-written extensions to Cisco Access Registrar. An incoming script can examine and change the attributes of the request packet or the environment variables, which can affect subsequent processing.

f. Based on the scripts or the defaults, it chooses a service to authenticate and/or authorize the user.

Step 4 Cisco Access Registrar's authentication service verifies the username and password is in its database. Or, Cisco Access Registrar delegates the authentication (as a proxy) to another RADIUS server, an LDAP, or TACACS server.

Step 5 Cisco Access Registrar's authorization service creates the response with the appropriate attributes for the user's session and puts it in the Response dictionary.

Step 6 If you are using Cisco Access Registrar session management at your site, the Session Manager calls the appropriate Resource Managers that allocate dynamic resources for this session.

Step 7 Cisco Access Registrar runs any outgoing scripts to change the attributes of the response packet.

Step 8 Cisco Access Registrar formats the response based on the Response dictionary and sends it back to the client (NAS).

Step 9 The NAS receives the response and communicates with the user, which may include sending the user an IP address to indicate the connection has been successfully established.

Types of RADIUS Messages

The client/server packet exchange consists primarily of the following types of RADIUS messages:

- Access-Request—sent by the client (NAS) requesting access
- Access-Reject—sent by the RADIUS server rejecting access
- Access-Accept—sent by the RADIUS server allowing access
- Access-Challenge—sent by the RADIUS server requesting more information in order to allow access. The NAS, after communicating with the user, responds with another Access-Request.

When you use RADIUS accounting, the client and server can also exchange the following two types of messages:

- Accounting-Request—sent by the client (NAS) requesting accounting
- Accounting-Response—sent by the RADIUS server acknowledging accounting

Packet Contents

The information in each RADIUS message is encapsulated in a UDP (User Datagram Protocol) data packet. A packet is a block of data in a standard format for transmission. It is accompanied by other information, such as the origin and destination of the data.

lists each message packet which contains the following five fields:

Table 1-1 ***RADIUS Packet Fields***

Fields	Description
Code	Indicates what type of message it is: Access-Request, Access-Accept, Access-Reject, Access-Challenge, Accounting-Request, or Accounting-Response.
Identifier	Contains a value that is copied into the server's response so the client can correctly associate its requests and the server's responses when multiple users are being authenticated simultaneously.
Length	Provides a simple error-checking device. The server silently drops a packet if it is shorter than the value specified in the length field, and ignores the octets beyond the value of the length field.

Table 1-1 ***RADIUS Packet Fields*** **(continued)**

Fields	Description
Authenticator	Contains a value for a Request Authenticator or a Response Authenticator. The Request Authenticator is included in a client's Access-Request. The value is unpredictable and unique, and is added to the client/server shared secret so the combination can be run through a one-way algorithm. The NAS then uses the result in conjunction with the shared secret to encrypt the user's password.
Attribute(s)	Depends on the type of message being sent. The number of attribute/value pairs included in the packet's attribute field is variable, including those required or optional for the type of service requested.

The Attribute Dictionary

The Attribute dictionary contains a list of preconfigured authentication, authorization, and accounting attributes that can be part of a client's or user's configuration. The dictionary entries translate an attribute into a value Cisco Access Registrar uses to parse incoming requests and generate responses. Attributes have a human-readable name and an enumerated equivalent from 1-255.

Sixty three standard attributes exist, which are defined in RFCs 2865, 2866, 2867, 2868, and 2869. There also are additional vendor-specific attributes that depend on the particular NAS you are using.

Some sample attributes include:

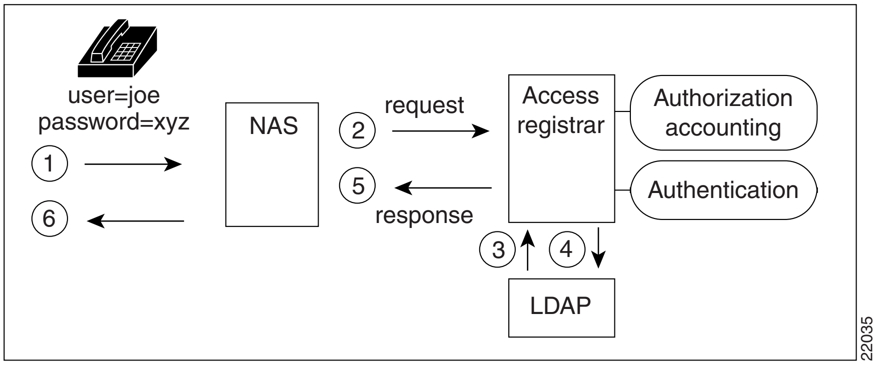
- User-Name—the name of the user
- User-Password—the user's password
- NAS-IP-Address—the IP address of the NAS
- NAS-Port—the NAS port the user is dialed in to
- Framed Protocol—such as SLIP or PPP
- Framed-IP-Address—the IP address the client uses for the session
- Filter-ID—vendor-specific; identifies a set of filters configured in the NAS
- Callback-Number—the actual callback number.

Proxy Servers

Any one or all of the RADIUS server's three functions: authentication, authorization, or accounting can be subcontracted to another RADIUS server. Cisco Access Registrar then becomes a *proxy server.* Proxying to other servers enables you to delegate some of the RADIUS server's functions to other servers.

You can use Cisco Access Registrar to "proxy" to an LDAP server for access to directory information about users in order to authenticate them. Figure 1-2 shows user `joe` initiating a request, the Cisco Access Registrar server proxying the authentication to the LDAP server, and then performing the authorization and accounting processing in order to enable `joe` to log in.

Figure 1-2 Proxying to an LDAP Server for Authentication



Basic Authentication and Authorization

This section provides basic information about how Cisco Access Registrar performs the basic RADIUS functions of authentication and authorization as defined in Internet RFC 2865.

- Authentication—determining the identity of a user of a client NAS through user identification and password validation and deciding whether to grant access
- Authorization—determining the level of network services available to authenticated users after a connection has been established

The Cisco Access Registrar (AR) server provides authentication and authorization service to clients which are network access servers (NAS). The following paragraphs describe the steps to a connection.

1. The process begins when user dials into the NAS and enters a user name and a password. The NAS creates an Access-Request containing attributes such as the user's name, the user's password, the ID of the client, and the Port ID the user is accessing.
2. The Cisco AR server determines which hardware (client NAS) sent the request, parses the packet, and determines whether to accept the request.

   The Cisco AR server checks to see if the client's IP address is listed in **/Radius/Clients/<Name>/<IPAddress>**.
3. After accepting the request, the Cisco AR server does the following:
   - Sets up the Request Dictionary based on the packet information
   - Runs any incoming scripts (user-written extensions to Cisco Access Registrar)

     An incoming script can examine and change the attributes of the request packet or the environmental variables which can affect subsequent processing.
   - Based on default values or scripts, it chooses a service to authenticate and authorize the user.

     The Cisco AR server directs the request to the appropriate service, which then performs authentication and/or authorization according to the type specified in **/Radius/Services/<Name>/<Type>**.
   - Performs session management, directing the request to the appropriate Session Manager.

  - Performs resource management for each Resource Manager in the Session Manager. The Cisco AR server directs the request to the appropriate resource manager listed in **/Radius/SessionManagers/<Name>/<ResourceManagers>/<Name>**. The resource manager then allocates or checks the resource according to the type listed in **/Radius/<ResourceManagers>/<Name>/<Type>**.

4. The Cisco AR server finally creates and formats an Access-Accept, Access Reject, or Access Challenge response, then sends it to the client (NAS).

CHAPTER 2

Understanding Cisco Access Registrar

This chapter describes the Cisco Access Registrar object structure, and explains when Cisco Access Registrar references each of these objects during the processing of client requests.

Cisco Access Registrar lets you manipulate configuration objects, which define the properties or behavior of the RADIUS server. Cisco Access Registrar also lets you invoke custom scripts to affect the behavior of the RADIUS server.

To better understand the role each of these objects plays in the program, it is helpful to look at the steps Cisco Access Registrar performs from receipt of an Access-Request packet to the sending of an Access-Response packet.

Cisco Access Registrar Hierarchy

Cisco Access Registrar's operation and configuration is based on a set of *objects*. These objects are arranged in a hierarchical structure much like the Windows 95 Registry or the UNIX directory structure. Cisco Access Registrar's objects can themselves contain subobjects, just as directories can contain subdirectories.

These objects include the following:

- Radius— the root of the configuration hierarchy
- UserLists—contains individual UserLists which in turn contain users
- UserGroups—contains individual UserGroups
- Clients—contains individual Clients
- Vendors—contains individual Vendors
- Scripts—contains individual Scripts
- Services—contains individual Services
- SessionManagers—contains individual Session Managers
- ResourceManagers—contains individual Resource Managers
- Profiles—contains individual Profiles
- RemoteServers—contains individual RemoteServers
- Advanced—contains Ports, Interfaces, Reply Messages, and the Attribute dictionary.

UserLists and Groups

Cisco Access Registrar lets you organize your user community through the configuration objects **UserLists**, **users**, and **UserGroups**.

- Use **UserLists** to group users by organization, such as Company A and Company B. Each list contains the actual names of the users.
- Use **users** to store information about particular users, such as name, password, group membership, base profile, and so on.
- Use **UserGroups** to group users by function, such as PPP, Telnet, or multiprotocol users. Groups allow you to maintain common authentication and authorization requirements in one place, and have them referenced by many users.

For more information about **UserLists** and **UserGroups**, refer to Access Registrar Server Objects in the *Cisco Access Registrar User's Guide*.

Profiles

Cisco Access Registrar uses **Profiles** that allow you to group RADIUS attributes to be included in an Access-Accept packet. These attributes include values that are appropriate for a particular user class, such as PPP or Telnet user. The user's base profile defines the user's attributes, which are then added to the response as part of the authorization process.

Although you can use Group or Profile objects in a similar manner, choosing whether to use one rather than the other depends on your site. If you require some choice in determining how to authorize or authenticate a user session, then creating specific profiles, and specifying a group that uses a script to choose among the profiles is more flexible. In such a situation, you might create a default group and then write a script that selects the appropriate profile based on the specific request. The benefit to this technique is each user can have a single entry, and use the appropriate profile depending on the way they log in.

For more information about **Profiles**, refer to Access Registrar Server Objects in the *Cisco Access Registrar User's Guide*.

Scripts

Cisco Access Registrar allows you to create scripts you can execute at various points within the processing hierarchy.

- Incoming scripts—enable you to read and set the attributes of the request packet, and set or change the Environment dictionary variables. You can use the environment variables to control subsequent processing, such as specifying the use of a particular authentication service.
- Outgoing scripts—enable you to modify attributes returned in the response packet.

For more information about **Scripts**, refer to Access Registrar Server Objects in the *Cisco Access Registrar User's Guide*.

Services

Cisco Access Registrar uses *Services* to let you determine how authentication, authorization, and/or accounting are performed.

For example, to use Services for authentication:

- When you want the authentication to be performed by the Cisco Access Registrar RADIUS server, you can specify the **local** service. In this, case you must specify a specific **UserList**.
- When you want the authentication performed by another server, which may run an independent application on the same or different host than your RADIUS server, you can specify either a **radius**, **ldap**, or **tacacs-udp** service. In this case, you must list these servers by name.

When you have specified more than one authentication service, Cisco Access Registrar determines which one to use for a particular Access-Request by checking the following:

- When an incoming script has set the Environment dictionary variable **Authentication-Service** with the name of a Service, Cisco Access Registrar uses that service.
- Otherwise, Cisco Access Registrar uses the default authentication service. The default authentication service is a property of the **Radius** object.

Cisco Access Registrar chooses the authentication service based on the variable **Authentication-Service**, or the default. The properties of that Service, specify many of the details of that authentication service, such as, the specific user list to use or the specific application (possibly remote) to use in the authentication process.

For more information about Services, refer to Access Registrar Server Objects in the *Cisco Access Registrar User's Guide*.

Session Management Using Resource Managers

Cisco Access Registrar lets you track user sessions, and/or allocate dynamic resources to users for the lifetime of their session. You can define one or more Session Managers, and have each one manage the sessions for a particular group or company.

Session Managers use Resource Managers, which in turn manage resources of a particular type as described below.

- IP-Dynamic—manages a pool of IP addresses and allows you to dynamically allocate IP addresses from that pool
- IP-Per-NAS-Port—allows you to associate ports to specific IP addresses, and thus ensure each NAS port always gets the same IP address
- IPX-Dynamic—manages a pool of IPX network addresses
- Group-Session-Limit—manages concurrent sessions for a group of users; that is, it keeps track of how many sessions are active and denies new sessions once the configured limit has been reached
- User-Session-Limit—manages per-user concurrent sessions; that is, it keeps track of how many sessions each user has and denies the user a new session once the configured limit has been reached
- USR-VPN—manages Virtual Private Networks (VPNs) that use USR NAS Clients.

For more information about Session Managers, refer to Access Registrar Server Objects in the *Cisco Access Registrar User's Guide*.

If necessary, you can create a complex relationship between the Session Managers and the Resource Managers.

When you need to share a resource among Session Managers, you can create multiple Session Managers that refer to the same Resource Manager. For example, if one pool of IP addresses is shared by two departments, but each department has a separate policy about how many users can be logged in concurrently, you might create two Session Managers and three Resource Managers. One dynamic IP Resource Manager that is referenced by both Session Managers, and two concurrent session Resource Managers, one for each Session Manager.

In addition, Cisco Access Registrar lets you pose queries about sessions. For example, you can query Cisco Access Registrar about which session (and thus which NAS-Identifier, NAS-Port and/or User-Name) owns a particular resource, as well as query Cisco Access Registrar about how many resources are allocated or how many sessions are active.

Cisco AR Directory Structure

The installation process populates the **/opt/CSCOar** directory with the subdirectories listed in Table 2-1.

Note This directory structure is different from that of previous version of Cisco AR.

Table 2-1 /opt/CSCOar Subdirectories

Subdirectory	Description
.system	Contains ELFs, or binary SPARC executables that should not be run directly
bin	Contains shell scripts and programs frequently used by a network administrator; programs that can be run directly
conf	Contains configuration files
data	Contains the **radius** directory, which contains session backing files; and the **db** directory, which contains configuration database files
examples	Contains documentation, sample configuration scripts, and shared library scripts
lib	Contains Cisco Access Registrar software library files
logs	Contains system logs and is the default directory for RADIUS accounting
odbc	Contains Cisco Access Registrar ODBC files
scripts	Contains sample scripts that you can modify to automate configuration, and to customize your RADIUS server
temp	Used for temporary storage
ucd-snmp	Contains the UCD-SNMP software Cisco Access Registrar uses
usrbin	Contains a symbolic link that points to **bin**.

Program Flow

When a NAS sends a request packet to Cisco Access Registrar with a name and password, Cisco Access Registrar performs the following actions. Note, Table 2-2 describes the flow without regard to scripting points.

Table 2-2 From Access-Request to Access-Accept

Cisco AR Server Action	Explanation
Receives an Access-Request	The Cisco Access Registrar server receives an Access-Request packet from a NAS
Determines whether to accept the request	The Cisco Access Registrar server checks to see if the client's IP address is listed in **/Radius/Clients/**<*Name*>**/**<*IPAddress*>
Invokes the policy SelectPolicy if it exists	The Cisco ARPolicy Engine provides an interface to define and configure a policy and to apply the policy to the corresponding access-request packets
Performs authentication and/or authorization	Directs the request to the appropriate service, which then performs authentication and/or authorization according to the type specified in **/Radius/Services/**<*Name*>**/**<*Type*>
Performs session management	Directs the request to the appropriate Session Manager
Performs resource management for each Resource Manager in the SessionManager	Directs the request to the appropriate resource manager listed in **/Radius/SessionManagers/**<*Name*>**/**<*ResourceManagers*>**/**<*Name*>, which then allocates or checks the resource according to the type listed in **/Radius/**<*ResourceManagers*>**/**<*Name*>**/**<*Type*>
Sends an Access-Accept	Creates and formats the response, and sends it back to the client (NAS)

Scripting Points

Cisco Access Registrar lets you invoke scripts you can use to affect the Request, Response, or Environment dictionaries.

Client or NAS Scripting Points

Table 2-3 shows the location of the scripting points within the section that determines whether to accept the request from the client or NAS. Note, the scripting points are indicated with the asterisk (*) symbol.

Table 2-3 Client or NAS Scripting Points

Action	Explanation
Receives an Access-Request.	The Cisco Access Registrar RADIUS server receives an Access-Request packet from a NAS.
Determines whether to accept the request.	The client's IP address listed in **/Radius/Clients/**<*Name*>**/IPAddress**.
*Executes the server's incoming script.	A script referred to in **/Radius/IncomingScript**.
*Executes the vendor's incoming script.	The vendor listed in /Radius/Clients/*Name*/Vendor, and is a script referred to in **/Radius/Vendors/**<*Name*>**/IncomingScript**.
*Executes the client's incoming script.	A script referred to in **/Radius/Clients/**<*Name*>**/IncomingScript**.
Determines whether to accept requests from this specific NAS.	

Table 2-3 Client or NAS Scripting Points (continued)

Action	Explanation
	/Radius/Advanced/RequireNASsBehindProxyBeInClientList set to TRUE.
	The NAS's Identifier listed in **/Radius/Clients/**<*Name*>, or its NAS-IP-Address listed in **/Radius/Clients/**<*Name*>**/IPAddress**.
If the client's IP address listed in /Radius/Clients/<*Name*>**/IPAddress is different:**	
*Executes the vendor's incoming script.	The vendor listed in **/Radius/Clients/***Name*/Vendor, and is a script referred to in **/Radius/Vendors/**<*Name*>**/IncomingScript**.
*Executes the client's incoming script.	The client listed in the previous /Radius/Clients/*Name*, and is a script referred to in /Radius/Clients/*Name*/IncomingScript.

Authentication and/or Authorization Scripting Points

Table 2-4 shows the location of the scripting points within the section that determines whether to perform authentication and/or authorization.

Table 2-4 Authentication and Authorization Scripting Points

Action	Explanation
Determines Service to use for authentication and/or authorization.	The Service name defined in the Environment dictionary variable **Authentication-Service**, and is the same as the Service defined in the Environment dictionary variable **Authorization-Service**.
	The Service name referred to by **/Radius/DefaultAuthenticationService**, and is the same as the Service defined in **/Radius/DefaultAuthorizationService**.
Performs authentication and/or authorization.	If the Services are the same, perform authentication and authorization.
	If the Services are different, just perform authentication.
*Executes the Service's incoming script.	A script referred to in **/Radius/Services/**<*Name*>**/IncomingScript**.
Performs authentication and/or authorization.	Based on the Service type defined in **/Radius/Services/**<*Name*>**/**<*Type*>.
*Executes the Service's outgoing script.	A script referred to in **/Radius/Services/**<*Name*>**/OutgoingScript**.

Action	Explanation
Determines whether to perform authorization.	The Service name defined in **/Radius/DefaultAuthorizationService**, if different than the Authentication Service.
*Executes the Service's incoming script.	A script referred to in **/Radius/Services/**<*Name*>**/IncomingScript**.
Performs authorization.	Checks that the Service type is defined in **/Radius/Services/**<*Name*>**/**<*Type*>.
*Executes the Service's outgoing script.	A script referred to in **/Radius/Services/**<*Name*>**/OutgoingScript**.

Session Management

The Session Management feature requires the client (NAS or proxy) to send all RADIUS accounting requests to the Cisco Access Registrar server performing session management. (The only exception is if the clients are USR/3Com Network Access Servers configured to use the USR/3Com RADIUS resource management feature.) This information is used to keep track of user sessions, and the resources allocated to those sessions.

When another accounting RADIUS server needs this accounting information, the Cisco Access Registrar server performing session management may proxy it to this second server.

Table 2-5 describes how Cisco Access Registrar handles session management.

Table 2-5 Session Management Processing

Action	Explanation
Determines whether to perform session management.	The session management defined in the Environment dictionary variable **Session-Manager**.
	The session management name referred to in **/Radius/DefaultSessionManager**.
Performs session management.	Selects Session Manager as defined in **/Radius/SessionManagers/**<*Name*>.
Performs resource management.	Directs the request to the appropriate Resource manager listed in **/Radius/SessionManagers/**<*Name*>**/ResourceManagers/**<*Name*>, which then allocates or checks the resource according to the type listed in **/Radius/ResourceManagers/**<*Name*>**/**<*Type*>.
Sends an Access-Accept.	Creates and formats the response, and sends it back to the client (NAS).

Failover by the NAS and Session Management

When a Network Access Server's primary RADIUS server is performing session management, and the NAS determines the server is not responding and begins sending requests to its secondary RADIUS server, the following occurs:

- The secondary server will not know about the current active sessions that are maintained on the primary server. Any resources managed by the secondary server must be distinct from those managed by the primary server, otherwise it will be possible to have two sessions with the same resources (for example, two sessions with the same IP address).
- The primary server will miss important information that allows it to maintain a correct model of what sessions are currently active (because the authentication and accounting requests are being sent to the secondary server). This means when the primary server comes back online and the NAS begins using it, its knowledge of what sessions are active will be out-of-date and the resources for those sessions are allocated even if they are free to allocate to someone else.

  For example, the user-session-limit resource may reject new sessions because the primary server does not know some of the users using the resource logged out while the primary server was off-line. It may be necessary to release sessions manually using the **aregcmd** command **release-session**.

Note It may be possible to avoid this situation by having a disk drive shared between two systems with the second RADIUS server started up once the primary server has been determined to be off-line. For more information on this setup, contact Technical Support.

Script Processing Hierarchy

For request packets, the script processing order is from the most general to the most specific. For response packets, the processing order is from the most specific to the most general.

Table 2-6, Table 2-7, and Table 2-8 show the overall processing order and flow:
(1-6) Incoming Scripts, (7-11) Authentication/Authorization Scripts, and (12-17) Outgoing Scripts.

Note The client and the NAS can be the same entity, except when the immediate client is acting as a proxy for the actual NAS.

Table 2-6 Cisco Access Registrar Processing Hierarchy for Incoming Scripts

Overall Flow Sequence	Incoming Scripts
1)	Radius
2)	Vendor of the immediate client.
3)	Immediate client.
4)	Vendor of the specific NAS.
5)	Specific NAS
6)	Service

Table 2-7 Cisco Access Registrar Processing Hierarchy for Authentication/Authorization Scripts

Overall Flow Sequence	Authentication/Authorization Scripts
7)	Group Authentication.
8)	User Authentication.
9)	Group Authorization.

Overall Flow Sequence	Authentication/Authorization Scripts
10)	User Authorization.
11)	Session Management.

Table 2-8 Cisco Access Registrar Processing Hierarchy for Outgoing Scripts

Overall Flow Sequence	Outgoing Scripts
12)	Service
13)	Specific NAS.
14)	Vendor of the specific NAS.
15)	Immediate client.
16)	Vendor of the immediate client.
17)	Radius

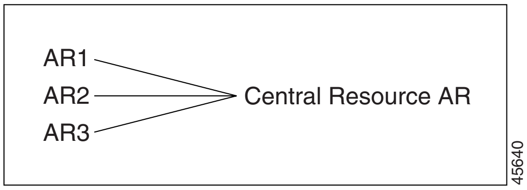
Cross Server Session and Resource Management

Prior to Cisco AR1.6, sessions and resources were managed locally, meaning that in a multi-AR server environment, resources such as IP addresses, user-based session limits, and group-based session limits were divided between all the Cisco ARservers. It also meant that, to ensure accurate session tracking, all packets relating to one user session were required to go to the same Cisco ARserver.

Overview

Cisco Access Registrar 1.6 and above can manage sessions and resources across AAA server boundaries. A session can be created by an Access-Request sent to AR1, and it can be removed by an Accounting-Stop request sent to AR2, as shown in Figure 2-1. This enables accurate tracking of User and Group session L across multiple AAA servers, and IP addresses allocated to sessions are managed in one place.

Figure 2-1 Multiple Cisco AR Servers



All resources that must be shared cross multiple front line Cisco AR servers are configured in the Central Resource Cisco AR server. Resources that are not shared can still be configured at each front line Cisco AR server as done prior to the Cisco AR 1.6 release.

When the front line Cisco AR server receives the access-request, it does the regular AA processing. If the packet is not rejected and a Central Resource Cisco AR server is also configured, the front line Cisco AR server will proxy the packet[1] to the configured Central Resource Cisco AR. If the Central Resource Cisco AR server returns the requested resources, the process continues to the local session management (if local session manager is configured) for allocating any local resources. If the Central Resource Cisco AR server cannot allocate the requested resource, the packet is rejected.

When the Accounting-Stop packet arrives at the frontline Cisco AR, it does the regular accounting processing. Then, if the front line Cisco AR server is configured to use Central Resource Cisco AR, a proxy packet will be sent to Central Resource Cisco AR server for it to release all the allocated resources for this session. After that, any locally allocated resources are released by the local session manager.

Session-Service Service Step and Radius-Session Service

A new Service step has been added in the processing of Access-Request and Accounting packets. This is an additional step after the AA processing for Access packet or Accounting processing for Accounting packet, but before the local session management processing. The Session-Service should have a service type of Radius-Session.

An environment variable Session-Service is introduced to determine the Session-Service dynamically. You can use a script or the policy engine to set the Session-Service environment variable.

Configuring a Front Line Cisco Access Registrar

To use a Central Resource server, the DefaultSessionService property must be set or the Session-Service environment variable must be set through a script or the policy engine. The value in the Session-Service variable overrides the DefaultSessionService.

The configuration parameters for a Session-Service service type are the same as those for configuring a radius service type for proxy, except the service type is ***radius-session***.

The configuration for a Session-Service Remote Server is the same as configuring a proxy server.

```
[ //localhost/Radius ]
    Name = Radius
    Description =
    Version = 1.7R0
    IncomingScript =
    OutgoingScript =
    DefaultAuthenticationService = local-users
    DefaultAuthorizationService = local-users
    DefaultAccountingService = local-file
    DefaultSessionService = Remote-Session-Service
    DefaultSessionManager = session-mgr-1


[ //localhost/Radius/Services ]
    Remote-Session-Service/
       Name = Remote-Session-Service
       Description =
       Type = radius-session
```

[1] The proxy packet is actually a resource allocation request, not an Access Request.

```
       IncomingScript =
       OutgoingScript =
       OutagePolicy = RejectAll
       OutageScript =
       MultipleServersPolicy = Failover
       RemoteServers/
         1. central-server

[ //localhost/Radius/RemoteServers ]
    central-server/
       Name = central-server
       Description =
       Protocol = RADIUS
       IPAddress = 209.165.200.224
       Port = 1645
       ReactivateTimerInterval = 300000
       SharedSecret = secret
       Vendor =
       IncomingScript =
       OutgoingScript =
       MaxTries = 3
       InitialTimeout = 2000
       AccountingPort = 1646
```

Configure Central AR

Resources at the Central Resource server are configured the same way as local resources are configured. These resources are local resources from the Central Resource server’s point of view.

CHAPTER 3

Cisco Access Registrar Scripts

This chapter describes the scripts provided with Cisco Access Registrar.

Using Cisco AR Scripts

The Cisco Access Registrar scripts are stored in **/localhost/Radius/Scripts**. Most of the scripts are written in the RADIUS Extension language (REX). Some scripts are provided in both REX and Tcl. The scripts written in Tcl all begin with the letter **t** followed by their functional name. The Tcl scripts are listed below:

tACMEOutgoingScript
tAuthorizePPP
tAuthorizeService
tAuthorizeTelnet
tMapSourceIPAddress
tParseAARealm
tParseAASRealm
tParseProxyHints
tParseServiceAndAAARealmHints
tParseServiceAndAAASRealmHints
tParseServiceAndAARealmHints
tParseServiceAndAASRealmHints
tParstSericeAndProxyHints
tParseServiceHints

ACMEOutgoingScript

ACMEOutgoingScript is referenced from Vendor ACME for the outgoing script. If the Cisco AR server accepts this Access-Request and the response does not yet contain a Session-Timeout, set it to 3600 seconds.

AltigaIncomingScript

AltigaIncomingScript maps Altiga-proprietary attributes to Cisco Access Registrar’s global attribute space.

AltigaOutgoingScript

AltigaOutgoingScript maps Altiga attributes from Cisco Access Registrar's global attribute space to the appropriate Altiga-proprietary attributes.

ANAAAOutgoing

ANAAAOutgoing can be referenced from either the client or vendor outgoing scripting point to be used in HRPD/EV-DO networks where Cisco Access Registrar is the Access Network (AN) AAA server. ANAAAOutgoing checks to see if the response contains the Callback-Id attribute. If the response contains the Callback-Id attribute and the value is less than 253 characters, ANAAAOutgoing prefixes a zero (0) to the value. For example, it changes "123" into "0123." The ANAAAOutgoing script always returns REX_OK.

AscendIncomingScript

AscendIncomingScript maps Ascend-proprietary attributes to Cisco Access Registrar's global attribute space.

AscendOutgoingScript

AscendOutgoingScript maps Ascend attributes from Cisco Access Registrar's global attribute space to the appropriate Ascend-proprietary attributes.

AuthorizePPP

AuthorizePPP is referenced from either the use record for users who's sessions are always PPP or from the from the script AuthorizeService, which checks the request to determine which service is desired. This script merges in the Profile named "default-PPP-users" into the response dictionary.

AuthorizeService

AuthorizeService is referenced from user record for users who's sessions might be PPP, SLIP or Telnet depending on how they are connecting to the NAS. This script checks the request to determine which service is desired. If it is telnet, it calls the script AuthorizeTelnet. If it is PPP, it calls the script AuthorizePPP. If it is SLIP, it calls the script AuthorizeSLIP. If it is none of these, it rejects the request.

AuthorizeSLIP

AuthorizeSLIP is referenced from either the user record for users who's sessions are always SLIP or from the from the script AuthorizeService, which checks the request to determine which service is desired. This script merges in the Profile named "default-SLIP-users" into the response dictionary.

AuthorizeTelnet

AuthorizeTelnet is referenced from either the user record for users who's sessions are always telnet or from the from the script AuthorizeService, which checks the request to determine which service is desired. This script merges in the Profile named "default-Telnet-users" into the response dictionary.

CabletronIncoming

CabletronIncoming maps Cabletron-proprietary attributes to Cisco Access Registrar's global attribute space.

CabletronOutgoing

Use CabletronOutgoing to map Cisco-proprietary attributes from Cisco Access Registrar's global attribute space to the appropriate Cabletron-proprietary attributes.

CiscoIncoming

Use CiscoIncoming to map Cisco-proprietary attributes to Cisco Access Registrar's global attribute space.

CiscoOutgoing

Use CiscoOutgoing to map Cisco-proprietary attributes from Cisco Access Registrar's global attribute space to the appropriate Cabletron-proprietary attributes.

CiscoWithODAPIncomingScript

Use CiscoWithODAPIncomingScript to map Cisco-proprietary attributes to Cisco Access Registrar's global attribute space and to map ODAP requests to the appropriate services and session managers.

CiscoWithODAPIncomingScript checks the incoming NAS-Identifier sent by the client. If the NAS-Identifier does not equal odap-dhcp, the request is not an ODAP request. If the request is not an ODAP request, the script does no more ODAP-specific processing, and calls CiscoIncomingScript to allow it to process the request.

If the request is an ODAP request, CiscoWithODAPIncomingScript removes the NAS-Identifier attribute because it is no longer required. The script then sets the Authentication-Service and the Authorization-Service to odap-users and sets the Accounting-Service to odap-accounting.

ExecCLIDRule

ExecCLIDRule is referenced from the policy engine to determine the authentication and authorization service and policy based on the CLID set in the policy engine.

ExecDNISRule

ExecDNISRule is referenced from the policy engine to determine the authentication and authorization service and policy based on the DNIS set in the policy engine.

ExecFilterRule

ExecFilterRule is referenced from the policy engine to determine whether a user packet should be rejected or not based on whether a special character like "*", "/", "\" or "?" shows up in the packet.

ExecNASIPRule

ExecNASIPRule is referenced from the policy engine to enable configuration of policies based on the incoming NAS-IP-Address. You can configure two attributes, *client-ip-address* and *subnetmask*, to match the incoming NAS-IP-Address and its subnet mask. If the attributes match, ExecNASIPrule sets the environment variables (if they are configured in that rule).

ExecRealmRule

ExecRealmRule is referenced from the policy engine to determine the authentication and authorization service and policy based on the realm set in the policy engine.

ExecTimeRule

ExecTimeRule either rejects or accepts Access Request packets based on the time range specified in a user's login profile. You can configure the TimeRange and AcceptedProfile attributes.

The format for the TimeRange is to set the allowable days followed by the allowable times, as in:

> TimeRange = dateRange, timeRange

The dateRange can be in the form of a date, a range of allowable dates, a day, or a range of allowable days. The timeRange should be in the form of hh:mm-hh:mm.

Here are a few examples:

mon-fri,09:00-17:00

> Allows access Monday through Friday from 9 AM until 5 PM.

mon,09:00-17:00;tue-sat,12:00-13:00

> Allows access on Monday from 9 AM until 5 PM and from 12 noon until 1 PM on Tuesday through Saturday

mon,09:00-24:00;tue,00:00-06:00

> Allows access on Monday from 9 AM until Tuesday at 6 AM

1-13,10-17:00; 15,00:00-24:00

> Allows access from the first of the month until the thirteenth of the month from 10 AM until 5 PM and all day on the fifteenth of the month.

LDAPOutage

LDAPOutage is referenced from LDAP Services as OutageScript. LDAPOutage logs when the LDAP binding is lost.

MapSourceIPAddress

MapSourceIPAddress is referenced from the Cisco Access Registrar server's IncomingScript scripting point. MapSourceIPAddress checks to see if the request contains either a NAS-Identifier or a NAS-IP-Address. If not, this script sets the NAS-IP-Address from the request's source IP address.

The Tcl version of this script is tMapSourceIPAddress.

ParseAAARealm

ParseAAARealm is referenced from the NAS IncomingScript scripting point. It looks for a realm name on the user name attribute as a hint of which AAA service should be used for this request. If @<realm> is found, the AAA service is selected which has the same name as the realm.

ParseAAASRealm

ParseAAASRealm is referenced from the NAS incoming script extension point. ParseAAASRealm looks for a realm name on the user name attribute as a hint of which AAA service and which SessionManager should be used for this request. If @<realm> is found, the AAA service and SessionManager which have the same name as the realm are selected.

ParseAARealm

ParseAARealm is referenced from the NAS IncomingScript scripting point. It looks for a realm name on the user name attribute as a hint of which authentication and authorization service should be used for this request. If @<realm> is found, it selects the AA service that has the same name as the realm and the DefaultAccountingService (as specified in the configuration by the administrator).

The Tcl version of this script is named tParseAARealm.

ParseAASRealm

ParseAASRealm is referenced from the NAS IncomingScript scripting point. It looks for a realm name on the user name attribute as a hint of which AA service and which SessionManager should be used for this request. If @<realm> is found, the AA service and the SessionManager which have the same name as the realm are selected. The Accounting service will be the DefaultAccountingService (as specified in the configuration by the administrator).

The Tcl version of this script is named tParseAASRealm.

ParseProxyHints

ParseProxyHints is referenced from the NAS IncomingScript scripting point. It looks for a realm name on the user name attribute as a hint of which AAA services should be used for this request. If @radius is found, a set of AAA services is selected which will proxy the request to a remote radius server. If @tacacs is found, the AuthenticationService is selected that will proxy the request to a tacacs server for authentication. For any services not selected, the default service (as specified in the configuration by the administrator) will be used.

The Tcl version of this script is named tParseProxyHints.

ParseServiceAndAAARealmHints

ParseServiceAndAAARealmHints is referenced from the NAS IncomingScript scripting point. It calls both ParseServiceHints and ParseAAARealm.

The Tcl version of this script is named tParseServiceAndAAARealmHints.

ParseServiceAndAAASRealmHints

ParseServiceAndAAASRealmHints is referenced from the NAS IncomingScript scripting point. It calls both ParseServiceHints and ParseAAASRealm.

The Tcl version of this script is named tParseServiceAndAAASRealmHints.

ParseServiceAndAARealmHints

ParseServiceAndAARealmHints is referenced from the NAS IncomingScript scripting point. It calls both ParseServiceHints and ParseAARealm.

The Tcl version of this script is named tParseServiceAndAARealmHints.

ParseServiceAndAASRealmHints

ParseServiceAndAASRealmHints is referenced from the NAS IncomingScript scripting point. It calls both ParseServiceHints and ParseAASRealm.

The Tcl version of this script is named tParseServiceAndAASRealmHints.

ParseServiceAndProxyHints

ParseServiceAndProxyHints is referenced from the NAS IncomingScript scripting point. It calls both ParseServiceHints and ParseProxyHints.

The Tcl version of this script is named tParseServiceAndProxyHints.

ParseServiceHints

ParseServiceHints is referenced from the NAS IncomingScript scripting point. Check to see if we are given a hint of the service type or the realm. If so, set the appropriate attributes in the request or radius dictionary to record the hint and rewrite the user name to remove the hint.

The Tcl version of this script is named tParseServiceHints.

ParseTranslationGroupsByCLID

ParseTranslationGroupsByCLID is referenced from the policy engine to determine the incoming and outgoing translation groups based on CLID set in the policy engine so that the attributes can be added and/or filtered out by the configuration data set in MCD.

ParseTranslationGroupsByDNIS

ParseTranslationGroupsByDNIS is referenced from the policy engine to determine the incoming and outgoing translation groups based on realm set in the policy engine so that the attributes can be added/filtered out by the configuration data set in MCD.

ParseTranslationGroupsByRealm

ParseTranslationGroupsByRealm is referenced from the policy engine to determine the incoming and outgoing translation groups based on the realm set in the policy engine. ParseTranslationGroupsByRealm allows the attributes to be added or filtered out by the configuration data set in MCD.

UseCLIDAsSessionKey

UseCLIDAsSessionKey is used to specify that the Calling-Station-Id attribute should be used as the session key to correlate requests for the same session. This is a typical case for 3G mobile user session correlation.

USRIncomingScript

USRIncomingScript maps USR-proprietary attributes to Cisco Access Registrar’s global attribute space.

USRIncomingScript-IgnoreAccountingSignature

USRIncomingScript-IgnoreAccountingSignature maps USR-proprietary attributes to Cisco Access Registrar’s global attribute space and sets a flag to ignore the signature on Accounting-Request packets. Earlier versions of the USR RADIUS client did not correctly sign Accounting-Request packets.

USROutgoingScript

USROutgoingScript maps USR attributes from Cisco Access Registrar's global attribute space to the appropriate USR-proprietary attributes.

CHAPTER 4

Understanding Replication

This chapter describes Cisco Access Registrar's configuration replication features, functions, limitations and operation.

Replication Overview

Cisco Access Registrar replication feature can maintain identical configurations on multiple machines simultaneously. When replication is properly configured, changes an administrator makes on the primary or *master* machine are propagated by Cisco Access Registrar to a secondary or *slave* machine.

Replication eliminates the need to have administrators with multiple Cisco Access Registrar installations make the same configuration changes at each of their installations. Instead, only the master's configuration need be changed and the slave is automatically configured eliminating the need to make repetitive, error-prone configuration changes for each individual installation. In addition to enhancing server configuration management, using replication eliminates the need for a hot-standby machine.

Using a hot-standby machine is a common practice to provide more fault-tolerance where a fully-installed and configured system stands ready to takeover should the primary machine fail. However, a system setup for hot-standby is essentially an idle machine only used when the primary system fails. Hot-standby or secondary servers are expensive resources. Employing Cisco Access Registrar's replication feature, both servers may perform RADIUS request processing simultaneously, eliminating wasted resources.

The replication feature focuses on configuration maintenance only, not session information or installation-specific information such as Administrator, Interface, Replication or Advanced machine-specific configuration changes. These configuration items are not replicated because they are specific to each installation and are not likely to be identical between master and slave. While changes to Session Managers, Resource Manager, and Remote Servers are replicated to the slave and stored in the slave's configuration database, they are not hot-configured on the slave (see Hot Configuration Detailed below for more information)

Changes should be made only on the master server. Making changes on a slave server will not be replicated and may result in an unstable configuration on the slave. Any changes made using replication will not be reflected in existing **aregcmd** sessions. **aregcmd** only loads its configuration at start up; it is not dynamically updated. For example, if **aregcmd** is running on the slave, and on the master **aregcmd** is used to add a client, the new client, while correctly replicated and hot-configured, will not be visible in the slave's **aregcmd** until **aregcmd** is exited and restarted.

When there is a configuration change, the master server propagates the change set to all member servers over the network. All member servers have to update their configuration after receiving the change set notifications from master server. Propagating the change set to a member serve involves multiple packet transfer from the master server to the member because the master serve has to convey all the configuration changes to the member. The number of packets to be transferred depends on the size of the change set.

After receiving a change set notification, the member server will go off-line before applying the change set received from master server. This state is indicated by the log message `Radius Server is Off-line` in **name_radius_1_log** file. When the change set is successfully applied, the member server goes up automatically. This is indicated by the log message `Radius Server is On-Line` in **name_radius_1_log** file. When the member server goes off-line to apply the change set, no incoming packets are processed.

Due to the number of packets to be transferred in the change set and the amount of time the member server will be offline updating its databasepoints, Cisco recommends that you use multiple **save** commands rather than a large configuration change with one **save** command. You can also minimize the number of changes that occur in a replication interval by modifying either the RepTransactionArchiveLimit or the RepTransactionSyncInterval, or both of these properties. For example, instead of using the default value of 100 for the RepTransactionArchiveLimit, you might change it to 20.

How Replication Works

This section describes the flow of a simple replication as it occurs under normal conditions.

Replication Data Flow

The following sections describe data flow on the master server and the slave server.

Master Server

The following describes the data flow for the master server:

Step 1 The administrator makes a change to the master server's configuration using the **aregcmd** command line interface (CLI) and issues a **save** command.

Step 2 After the changes are successfully validated, the changes are stored in the Access Registrar database.

Step 3 **aregcmd** then notifies the Access Registrar server executing on the master of the configuration change.

Step 4 The Access Registrar server then updates its version of the configuration stored in memory. (This is called *hot-config* because it happens while the server is running and processing requests.)

Step 5 The Access Registrar server first copies the changes pertaining to the **aregcmd save**, also known as a transaction to its replication archive, then transmits the transaction to the slave server for processing.

Step 6 In **aregcmd**, the prompt returns indicating that the **save** has completed successfully, the transaction has been archived, and the transaction has been transmitted to the slaves.

Slave Server

Step 1 When the slave server receives the transaction, its contents are verified.

Step 2 Once verified, the changes are applied to the slave server's database

Step 3 The changes are then applied (hot-configured) in the slave server's in-memory configuration.

Step 4 The transaction is written to the slave server's replication archive.

Security

Replication has two primary security concerns:

- Security of the transactions transmitted to the slave server
- Storage of transactions in the replication archive

Both of these concerns use shared secret (MD5) encryption via the shared secret specified in the replication configuration on both master and slave servers. Replication data transmitted between master and slave is encrypted at the source and decrypted at the destination the same way as standard RADIUS packets between Access Registrar's clients and the Access Registrar server. Transactions written to the replication archive are also encrypted in the same manner and decrypted when read from the replication archive.

Replication Archive

The replication archive serves two primary purposes:

1. To provide persistent, or saved, information regarding the last successful transaction
2. To persist transactions in case the slave server requires re synchronization (see Ensuring Data Integrity below for more information on re synchronization).

The replication archive is simply a directory located in **../CSCOar/data/archive**. Each transaction replicated by the master is written to this directory as a single file. The name of each transaction file is of the form txn########## where ########## is the unique transaction number assigned by the master server. The replication archive size, that is the number of transaction files it may contain, is configured in the Replication configuration setting of TransactionArchiveLimit. When the TransactionArchive limit is exceeded, the oldest transaction file is deleted.

Ensuring Data Integrity

Access Registrar's configuration replication feature ensures data integrity through transaction data verification, transaction ordering, automatic resynchronization and manual full-resynchronization. With the single exception of a manual full-resynchronization, each of the following techniques help to automatically ensure that master and slave servers contain identical configurations. A detailed description of each technique follows.

Transaction Data Verification

When the master prepares a transaction for replication to a slave, the master calculates a 2's complement Cyclic Redundancy Check (CRC) for each element (individual configuration change) in the transaction and for the entire transaction and includes these CRC values in the transmitted transaction. When the slave receives the transaction, the slave calculates a CRC for each transaction element and for the entire transaction and compares its own calculated values with those sent with the message. If a discrepancy occurs from these comparisons, the transaction element or the entire transaction is discarded and a re-transmission of that particular transaction element or the entire transaction is requested by the slave from the master. This process is called automatic resynchronization. (described in more detail below)

Transaction Order

When the master prepares a transaction for replication, it assigns the transaction a unique transaction number. This number is used to ensure the transactions are processed by the slave in exactly the same order as they were processed on the master. Transactions are order dependent. Since the functionality of Access Registrar's configuration replication feature is to maintain identical configurations between master and slave, if transaction order were not retained, master and slave would not contain identical configurations. Consider where two transactions modify the same thing (a defined client's IP address for example). If the first transaction was a mistake and the second was the desired result, the client config on the master would contain the second setting; however, if the transactions were processed in the reverse order on the slave, the client config on the slave would contain the mistaken IP Address. This example illustrates the critical need for transaction ordering to ensure data integrity.

Automatic Resynchronization

Automatic Resynchronization is the most significant feature with respect to data integrity. This feature ensures the configurations on both the master and slave are identical. If they are not, this feature automatically corrects the problem.

When the master and slave start-up, they determine the transaction number of the last replication transaction from their respective replication archives. The master immediately begins periodic transmission of a TransactionSync message to the slave. This message informs the slave of the transaction number of the transaction that the master last replicated.

If the transaction number in the TransactionSync message does not match the transaction number of the last received transaction in the slave's archive, then the slave will request resynchronization from the master. The resynchronization request sent by the slave will include the slave's last received transaction number.

The master will respond by retransmitting each transaction since the last transaction number indicated by the slave in the resynchronization request. The master obtains these transactions from its replication archive.

Should the slave's last received transaction number be less than the lowest transaction number in the master's replication archive, then automatic resynchronization cannot occur as the master's replication archive does not contain enough history to synchronize the slave. In this case, the slave must be resynchronized with a full-resynchronization.

Full Resynchronization

Full Resynchronization means that the slave has missed more transactions than are stored in the master's replication archive and cannot be resynchronized automatically. There is no automatic full-resynchronization mechanism in Access Registrar's configuration replication feature. To perform a full resynchronization, refer to the *Cisco Access Registrar User's Guide*.

Understanding Hot-Configuration

Hot-Configuration is the process of reflecting configuration changes made to Access Registrar's internal configuration database in the in-memory configuration of the executing Access Registrar server. Hot-Configuration is accomplished without interruption of RADIUS request processing. For example, if an administrator uses **aregcmd** to configure a new client and issues a **save** command, when the prompt returns, the newly configured client may send requests to Access Registrar.

Hot-Configuration minimizes the down-time associated with having to restart an Access Registrar server to put configuration changes into effect. With the Hot-Configuration feature, a restart is only necessary when a Session Manager, Resource Manager or Remote Server configuration is modified. These configuration elements may not be hot-configured because they maintain state (an active session, for example) and cannot be modified without losing the state information they maintain. Changes to these configuration elements require a restart of Access Registrar to put them into effect.

Hot-Configuration is not associated with the replication feature. Hot-Configuration's only connection to the replication feature is that when a change is replicated to the slave, the slave is hot-configured to reflect the replicated change as if an administrator had used **aregcmd** to make the changes directly on the slave server.

Replication's Impact on Request Processing

The replication feature was designed to perform replication of transactions with minimal impact on RADIUS request processing. When a transaction is received by a slave, RADIUS requests are queued while the transaction is applied to the slave. Once the transaction is complete, RADIUS request processing resumes.

The impact on RADIUS request processing is a direct result of the size of a transaction. The smaller the transaction the lesser the impact, and the larger the transaction, the greater the impact. In other words, when making changes to the master, frequent saves are better than making lots of changes and then saving. Each change is one transaction element and all changes involved in a **save** comprise a single transaction with one element per change. Since the replication feature only impacts RADIUS request processing when changes are made, the impact under normal operation (when changes are not being made) is virtually unmeasurable.

Replication Configuration Settings

This section describes each replication configuration setting. In **aregcmd**, replication settings are found in **//localhost/Radius/Replication**.

RepType

RepType indicates the type of replication. The choices available are SMDBR and NONE.

When RepType is set to NONE, replication is disabled. To enable replication, set RepType to SMDBR for Single Master DataBase Replication. RepType must be set to SMDBR on both the master and slave servers.

RepTransactionSyncInterval

Master

On the master server, RepTransactionSyncInterval is the duration between periodic transmission of the TransactionSync message expressed in milliseconds. The default is 60000 or 1 minute.

The purpose of RepTransactionSyncInterval is to indicate how frequently to check for an out-of -sync condition between the master and slave servers. When the slave received the TransactionSync message, it uses its contents to determine if it needs to resynchronize with the master.

The larger the setting for RepTransactionSyncInterval, the longer the period of time between out-of-sync detection. However, if RepTransactionSyncInterval is set too small, the slave may frequently request resynchronization when it is not really out of sync. If the duration is too small, the slave cannot completely receive a transaction before it receives the TransactionSync message. In this case, the servers will remain synchronized, but there will be unnecessary excess traffic that could affect performance.

Slave

On the slave, RepTransactionSyncInterval is used to determine if the slave has lost contact with the master and to alert administrators of a possible loss of connectivity between the master an slave. If the elapsed time since the last received TransactionSync message exceeds the setting of RepTransactionSyncInterval, the slave writes a log message indicating that it may have lost contact with the master. This log message is repeated each TransactionSyncInterval until a TransactionSync message is received.

RepTransactionArchiveLimit

On both master and slave, the RepTransactionArchiveLimit setting determines how many transactions can be stored in the archive. The default setting is 100. When the limit is exceeded, the oldest transaction file is deleted. If a slave requires resynchronization and the last transaction it received is no longer in the archive, a full resynchronization will be necessary to bring the slave back in sync with the master.

Note The value set for RepTransactionArchiveLimit should be the same on the master and the slave.

An appropriate value for RepTransactionArchiveLimit depends upon how much hard disk space an administrator can provide for resynchronization. If this value is large, say 10,000, then the last 10,000 transactions will be stored in the archive. This is like saying the last 10,000 saves from **aregcmd** will be stored in the archive. Large values are best. The size of each transaction depends upon how many configuration changes were included in the transaction, so hard disk space usage is difficult to estimate.

If the slave should go down or otherwise be taken off line, the value of RepTransactionArchiveLimit and the frequency of **aregcmd** saves will determine how long the slave may be off-line before a full-resynchronization will be required.

There are two reasons why a slave server should have an archive:

1. The slave must save the last received transaction for resynchronization purposes (at a minimum).
2. Should the master go down, the slave can then be configured as the master and provide resynchronization services to other slaves.

RepIPAddress

The RepIPAddress value is set to the IP Address of the machine containing the Access Registrar installation.

RepPort

The RepPort is the port used to receive of replication messages. In most cases, the default value (1645) is sufficient. If another port is to be used, the interfaces must exist in the machine.

RepSecret

RepSecret is the replication secret shared between the master and slave. The value of this setting must be identical on both the master and the slave.

RepIPMaster

The RepIPMaster setting indicates whether the machine is a master or a slave. On the master, set RepIPMaster to TRUE. On the slave set it to FALSE. Only the master may have this value set to TRUE and there can be only one master.

RepMasterIPAddress

RepMasterIPAddress specifies the IP Address of the master. On the master, set RepMasterIPAddress to the same value used in RepIPAddress above. On the slave, RepMasterIPAddress must be set to the IP Address of the master.

RepMasterPort

RepMasterPort is the port to use to send replication messages to the master. In most cases, the default value (1645) is sufficient; however, if another is to be used, the interfaces must exist in the machine.

Rep Members Subdirectory

The Rep **Members** subdirectory contains the list of slaves to which the master will replicate transactions.

Rep Members/Slave1

Each slave is added much like a client is added. Each slave must have a configuration in the Rep Members directory to be considered part of the *replication network* by the master. The master will not transmit any messages or replications to servers not in this list, and any communication received by a server not in this list will be ignored.

Note Although it is possible to configure multiple slaves with the same master, we have only considered a single-master/single-slave configuration. This is the recommended configuration.

Name

This is the name of the slave. The name must be unique.

IPAddress

This is the IP Address of the slave.

Port

This is the port upon which the master will send replication messages to the slave.

CHAPTER 5

Understanding SNMP

This chapter provides information about Cisco Access Registrar support for SNMP.

Overview

Cisco Access Registrar 3.0 provides SNMP MIB and trap support for users of network management systems. The supported MIBs enable the network management station to collect state and statistic information from an Cisco AR server. The traps enable Cisco AR to notify interested network management stations of failure or impending failure conditions.

Cisco Access Registrar supports the MIBs defined in the following RFCs:

- RADIUS Authentication Client MIB, RFC 2618
- RADIUS Authentication Server MIB, RFC 2619
- RADIUS Accounting Client MIB, RFC 2620
- RADIUS Accounting Server MIB, RFC 2621

Cisco Access Registrar 3.0 MIB support enables a standard SNMP management station to check the current state of the server as well as the statistics on each client or each proxied remote server.

Cisco Access Registrar 3.0 Trap support enables a standard SNMP management station to receive trap messages from an Cisco AR server. These messages contain information indicating that either the server was brought up or down, or that the proxied remote server is down or has come back online.

Supported MIBs

The MIBs supported by Access Registrar enable a standard SNMP management station to check the current state of the server and statistics for each client or proxied remote server.

RADIUS-AUTH-CLIENT-MIB

The RADIUS-AUTH-CLIENT-MIB describes the client side of the RADIUS authentication protocol. The information contained in this MIB is useful when an Cisco AR server is used as a proxy server.

RADIUS-AUTH-SERVER-MIB

The RADIUS-AUTH-SERVER-MIB describes the server side of the RADIUS authentication protocol. The information contained in this MIB describes managed objects used for managing a RADIUS authentication server.

RADIUS-ACC-CLIENT-MIB

The RADIUS-ACC-CLIENT-MIB describes the client side of the RADIUS accounting protocol. The information contained in this MIB is useful when an Cisco AR server is used for accounting.

RADIUS-ACC-SERVER-MIB

The RADIUS-ACC-CLIENT-MIB describes the server side of the RADIUS accounting protocol. The information contained in this MIB is useful when an Cisco AR server is used for accounting.

SNMP Traps

The traps supported by Access Registrar enable a standard SNMP management station to receive trap messages from an Cisco AR server. These messages contain information indicating whether a server was brought up or down, or that the proxied remote server is down or has come back online.

A trap is a network message of a specific format issued by an SNMP entity on behalf of a network management agent application. A trap is used to provide the management station with an asynchronous notification of an event.

When a trap is generated, a single copy of the trap is transmitted as a trap PDU to each destination contained within a list of trap recipients.

The list of trap recipients is shared by all events and is determined at server initialization time along with other trap configuration information. The list of trap recipients dictates where Cisco AR traps are directed.

The configuration of any other SNMP agent on the host is ignored. By default, all traps are enabled but no trap recipients are defined. By default, no trap is sent until trap recipients are defined.

Traps are configured using the command line interface (CLI). After configuring traps, the configuration information is re initialized when a server reload or restart occurs.

When you configure traps, you must provide the following information:

- List of trap recipients (community string for each)
- Suppressing traps for any type of message
- Frequency of traps for any type of message

Supported Traps

The traps supported by Cisco Access Registrar enable Cisco AR to notify interested management stations of events, failure, or impending failure conditions. Traps are a network message of a specific format issued by an SNMP entity on behalf of a network management agent application. Traps are used to provide the management station with an asynchronous notification of an event.

carServerStart

carServerStart signifies that the server has started on the host from which this notification was sent. This trap has one object, *carNotifStartType,* which indicates the start type. A *firstStart* indicates this is the server process' first start. *reload* indicates this server process has an internal reload. This typically occurs after rereading some configuration changes, but *reload* indicates this server process did not quit during the reload process.

carServerStop

carServerStop signifies that the server has stopped normally on the host from which this notification was sent.

carInputQueueFull

carInputQueueFull indicates that the percentage of use of the packet input queue has reached its high threshold. This trap has two objects:

- *carNotifInputQueueHighThreshold*—indicates the high limit percentage of input queue usage
- *carNotifInputQueueLowThreshold*—indicates the low limit percentage of input queue usage

By default, *carNotifInputQueueHighThreshold* is set to 90% and *carNotifInputQueueLowThreshold* is set to 60%.

Note The values for these objects cannot be changed at this time. You will be able to modify them in a future release of Cisco Access Registrar.

After this notification has been sent, another notification of this type will not be sent again until the percentage usage of the input queue goes below the low threshold.

If the percentage usage reaches 100%, successive requests may be dropped, and the server may stop responding to client requests until the queue drops down again.

carInputQueueNotVeryFull

carInputQueueNotVeryFull indicates that the percentage usage of the packet input queue has dropped below the low threshold defined in *carNotifInputQueueLowThreshold*. This trap has two objects:

- *carNotifInputQueueHighThreshold*—indicates the high limit percentage of input queue usage
- *carNotifInputQueueLowThreshold*—indicates the low limit percentage of input queue usage

After this type of notification has been sent, it will not be sent again until the percentage usage goes back up above the high threshold defined in *carNotifInputQueueHighThreshold*.

carOtherAuthServerNotResponding

carOtherAuthServerNotResponding indicates that an authentication server is not responding to a request sent from this server. This trap has three objects:

- *radiusAuthServerAddress—*indicates the identity of the concerned server
- *radiusAuthClientServerPortNumber—*indicates the port number of the concerned server
- *carAuthServerType*—indicates the type of the concerned server

The index of these three objects identifies the entry in *radiusAuthServerTable* and *carAccServerExtTable* which maintains the characteristics of the concerned server.

Note One should not rely solely on **carOtherAuthServerNotResponding** for server state. Several conditions, including a restart of the Cisco AR server, could result in either multiple *carOtherAuthServerNotResponding* notifications being sent or in a *carOtherAuthServerResponding* notification *not* being sent. NMS can query the *carAuthServerRunningState* in *carAuthServerExtTable* for the current running state of this server.

carOtherAuthServerResponding

carOtherAuthServerResponding signifies that an authentication server which had formerly been in a *down* state is now responding to requests from the Cisco AR server. This trap has three objects:

- *radiusAuthServerAddress—*indicates the identity of the concerned server
- *radiusAuthClientServerPortNumber—*indicates the port number of the concerned server
- *carAuthServerType*—indicates the type of the concerned server

The index of these three objects identifies the entry in *radiusAuthServerTable* and *carAccServerExtTable* which maintains the characteristics of the concerned server.

One should not rely on receiving this notification as an indication that all is well with the network. Several conditions, including a restart of the Cisco AR server, could result in either multiple *carOtherAuthServerNotResponding* notifications being sent or in a *carOtherAuthServerResponding* notification *not* being sent. The NMS can query the *carAuthServerRunningState* in *carAuthServerExtTable* for the current running state of this server.

carOtherAccServerNotResponding

carOtherAuthServerNotResponding signifies that an accounting server is not responding to the requests sent from this server. This trap has three objects:

- *radiusAccServerAddress—*indicates the identity of the concerned server
- *radiusAccClientServerPortNumber—*indicates the port number of the concerned server
- *carAcchServerType*—indicates the type of the concerned server

The index of these three objects identifies the entry in *radiusAuthServerTable* and *arAccServerExtTable* which maintains the characteristics of the concerned server.

One should not solely rely on this for server state. Several conditions, including the restart of the Cisco AR server, could result in either multiple *carOtherAccServerNotResponding* notifications being sent or in a *carOtherAccServerResponding* notification *not* being sent. The NMS can query the *carAccServerRunningState* in *carAccServerExtTable* for current running state of this server.

carOtherAccServerResponding

carOtherAccServerResponding signifies that an accounting server that had previously sent a *not responding* message is now responding to requests from the Cisco AR server. This trap has three objects:

- *radiusAccServerAddress*—indicates the identity of the concerned server
- *radiusAccClientServerPortNumber*—indicates the port number of the concerned server
- *carAccServerType*—indicates the type of the concerned server

The index of these three objects identifies the entry in *radiusAuthServerTable* and *arAccServerExtTable* which maintains the characteristics of the concerned server.

One should not rely on the reception of this notification as an indication that all is well with the network. Several conditions, including the restart of the Cisco AR server, could result in either multiple *carOtherAccServerNotResponding* notifications being sent or in a **carOtherAccServerResponding** notification *not* being sent. The NMS can query the *carAccServerRunningState* in *carAccServerExtTable* for the current running state of this server.

carAccountingLoggingFailure

carAccountingLoggingFailure signifies that this Cisco AR server cannot record accounting packets locally. This trap has two objects:

- *carNotifAcctLogErrorReason*—indicates the reason packets cannot be recorded locally
- *carNotifAcctLogErrorInterval*—indicates how long to wait until another notification of this type might be sent. A value of 0 (zero) indicates no time interval checking, meaning that no new notification can be sent until the error condition is corrected.

Configuring Traps

Cisco Access Registrar's SNMP implementation uses various configuration files to configure its applications.

Directories Searched

Configuration files can be found and read from numerous places. By default, SNMP applications look for configuration files in the following three directories (in the order listed):

1. **/usr/local/share/snmp/snmp.conf**

   This directory contains common configuration for the agent and the application. Refer to man page **snmp.conf(5)** for details.

2. **/usr/local/share/snmp/snmpd.conf**
3. **/usr/local/share/snmp/snmp.local.conf**

   This directory configures the agent. Refer to man page **snmp.conf(5)** for details.

In each of these directories, an SNMP application looks for files with the extension ***.conf***. The application also looks for configuration files in default locations where a configuration file can exist for any given configuration file type.

These files are optional and are only used to configure the extensible portions of the agent, the values of the community strings, and the optional trap destinations. By default, the first community string (“public” by default) is allowed read-only access and the second (“private” by default) is allowed write access, as well. The third to fifth community strings are also read-only.

Additionally, the above default search path can be over-ridden by setting the environmental variable SNMPCONFPATH to a colon-separated list of directories to search.

Finally, applications that store persistent data will also look for configuration files in the **/var/snmp** directory.

Configuration File Types

Each application may use multiple configuration files which will configure various different aspects of the application. For instance, the SNMP agent (**snmpd**) knows how to understand configuration directives in both the **snmpd.conf** and the **snmp.conf** files. In fact, most applications understand how to read the contents of the **snmp.conf** files. Note, however, that configuration directives understood in one file may not be understood in another file. For further information, read the associated manual page with each configuration file type. Also, most of the applications support a '-H' switch on the command line that will list the configuration files it will look for and the directives in each one that it understands.

The **snmp.conf** configuration file is intended to be a application suite-wide configuration file that supports directives that are useful for controlling the fundamental nature of all of the SNMP applications, such as how they all manipulate and parse the textual SNMP MIB files.

Switching Configuration Files in Mid-File

It's possible to switch in mid-file the configuration type that the parser is supposed to be reading. Since that output for the agent by default, but you didn't want to do that for the rest of the applications (for example, **snmpget** and **snmpwalk**, you would need to put a line like the following into the **snmp.conf** file.

```
dumpPacket true
```

But, this would turn it on for all of the applications. So, instead, you can put the same line in the snmpd.conf file so that it only applies to the snmpd demon. However, you need to tell the parser to expect this line. You do this by putting a special type specification token inside a square bracket ([ ]) set. In other words, inside your **snmpd.conf** file you could put the above **snmp.conf** directive by adding a line like the following:

```
[snmp] dumpPacket true
```

This tells the parser to parse the above line as if it were inside a **snmp.conf** file instead of an snmpd.conf file. If you want to parse a bunch of lines rather than just one then you can make the context switch apply to the remainder of the file or until the next context switch directive by putting the special token on a line by itself:

```
# make this file handle snmp.conf tokens:
[snmp]
dumpPacket true
logTimestamp true
# return to our original snmpd.conf tokens:
[snmpd]
rocommunity mypublic
```

Community String

A community string is used to authenticate the trap message sender (SNMP agent) to the trap recipient (SNMP management station). A community string is required in the list of trap receivers.

CHAPTER 6

Prepaid Billing Solution

This chapter describes the generic call flow between the three components required to support a prepaid billing solution using the RADIUS protocol: the AAA client, the Cisco Access Registrar 3.5 server, and a prepaid billing server.

Overview

When a subscriber uses a prepaid billing service, each call requires a set of data about the subscriber. However, the AAA network has no previous knowledge of the of the subscriber's usage behavior. To support the prepaid billing solution, Cisco AR 3.5 uses an iterative authorization paradigm over multiple sessions.

Each time an authorization request is made, the billing server apportions a fraction of the subscriber's balance into a quota. When a subscriber uses multiple sessions, each session must obtain its own quota. When a previously allocated quota is depleted, a session must be reauthorized to obtain a new quota.

Note The granularity and the magnitude of the quota is in the design and implementation of the prepaid billing server and is beyond the scope of this document. In general, a smaller the quota generates more network traffic, but allows more sessions per subscriber. When the quota is equal to a subscriber's total account balance, there is minimal network traffic, but only one session can be supported.

When a subscriber's current quota is depleted, the AAA client initiates a reauthorization request sending Access-Request packets. After the Cisco AR 3.5 server receives the request, it forwards the request to the billing server. The billing server then returns the next quota to use. The new quota might not be the same as the previous, and the billing server might adjust the quota dynamically.

Cisco Access Registrar 3.5 uses vendor-specific attributes (VSA) to extend the standard RADIUS protocol to carry information not usually present in the standard RADIUS packet. Cisco AR 3.5 uses a set of VSAs allocated to the Cisco VSA pool [26,9].

Cisco Access Registrar 3.5 required several different types of measurements to support a prepaid billing solution. These measurements require the use of metering variables to perform usage accounting. Table 6-1 lists the different measurements and what the AAA client, Cisco AR 3.5 server, and billing server do with them.

Table 6-1 Measurements and Component Actions

Measurement Type	Billing Server Action	AAA Server Action	AAA Client Action
Duration	Return duration quota	Convert duration quota to VSAs and pass along	Compare running duration quota with quota returned by Cisco AR 3.5 server
Total volume	Return volume quota	Convert volume quota to VSAs and pass along	Compare running volume quota with quota returned by Cisco AR 3.5 server
Uplink volume	Return volume quota	Convert volume quota to VSAs and pass along	Compare running volume quota with quota returned by Cisco AR 3.5 server
Downlink volume	Return volume quota	Convert volume quota to VSAs and pass along	Compare running volume quota with quota returned by Cisco AR 3.5 server
Total packets	Return packet quota	Convert packet quota to VSAs and pass along	Compare running packet quota with quota returned by Cisco AR 3.5 server
Uplink packets	Return packet quota	Convert packet quota to VSAs and pass along	Compare running packet quota with quota returned by Cisco AR 3.5 server
Downlink packets	Return packet quota	Convert packet quota to VSAs and pass along	Compare running packet quota with quota returned by Cisco AR 3.5 server
Logical OR of two measurements	Return quota of both measurements	Convert both to VSA and pass along	Monitor both quota and issue reauthorization packet when any one trips

Cisco AR 3.5 provides maximum flexibility to billing servers by allowing the metering variable to be modified as the service is used. This requires network nodes to measure all parameters all the time, but to report values only after receiving a reauthorization request.

Configuring Prepaid Billing

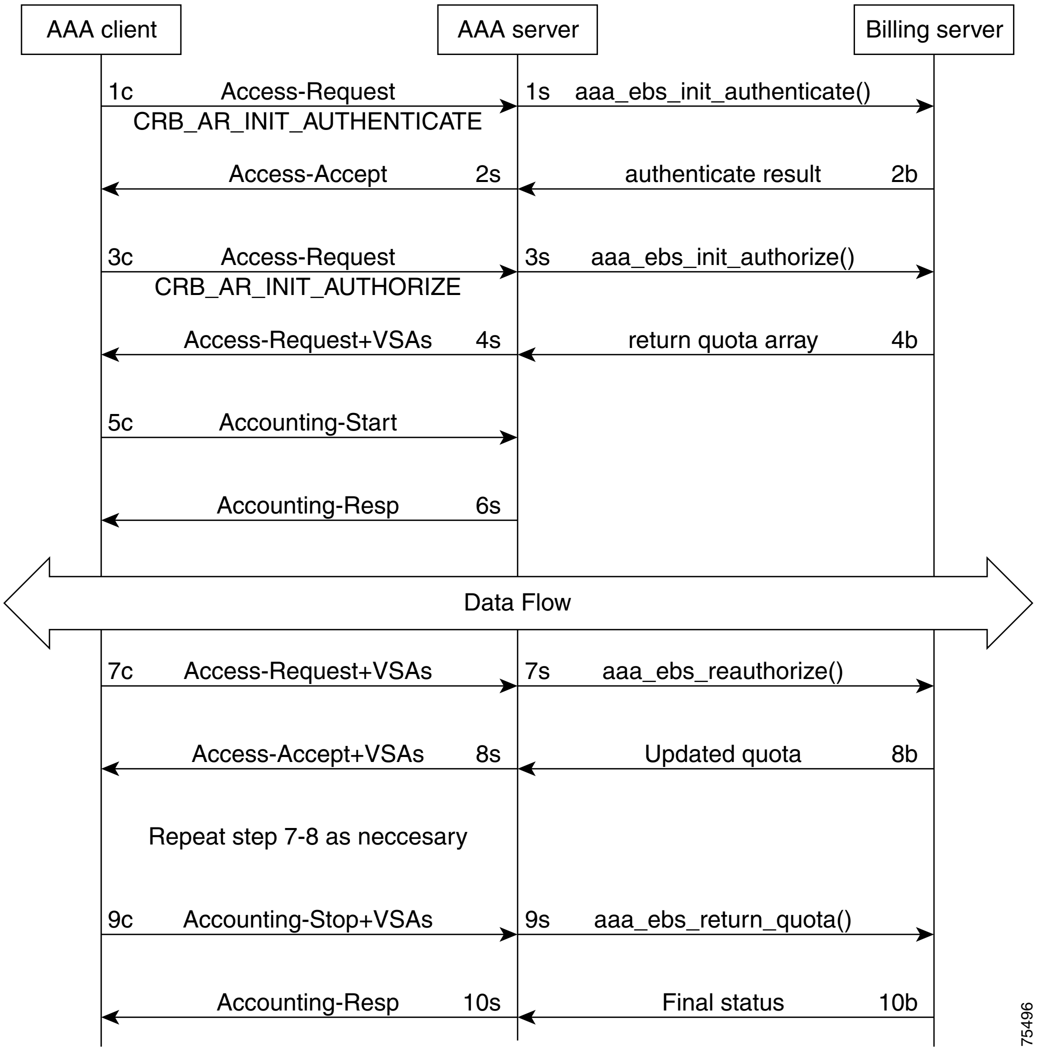
Cisco AR 3.5 uses a **prepaid** service to support prepaid billing solutions. A prepaid service has the following properties:

```
[ //localhost/Radius/Services/prepaid ]
    Name = prepaid
    Description =
    Type = prepaid
    IncomingScript~ =
    OutgoingScript~ =
    OutagePolicy~ = RejectAll
    OutageScript~ =
    MultipleServersPolicy = Failover
    RemoteServers/
```

Under RemoteServers, you must list the RemoteServer object previously configured to support either prepaid-crb or prepaid-is835c.

Detailed information about configuring prepaid billing is located in the *Cisco Access Registrar Installation and Configuration Guide*.

Figure 6-1 Generic Call Flow Diagram



Generic Call Flow

This section describes the generic call flow for the Cisco AR 3.5 prepaid billing solution. The call flow is controlled by the AAA client. The Cisco AR 3.5 server converts VSAs into calls to the billing server. The packet flows presented in Figure 6-1 are specific to the Cisco AR 3.5 prepaid billing solution only. The headlines in the packet flows are general and do represent all data transferred. The letters **c**, **s**, and **b** in Figure 6-1 designate the packet's source of **client**, **server**, or **billing server,** respectively.

Call Flow Details

This section provides details about the call flows and what each step achieves.

Note In the following attribute tables, entries beginning with APPL indicate application-specific attributes. Another application might use the field for different purpose or ignore the field. All the fields with APPL are specific to Mobile Wireless usage for illustration purpose.

Access-Request (Authentication)

Flow 1c shows the client sending the Access-Request to AAA server, part of a normal authentication request. The exact nature of the message contents is dictated by the access technology, be it be CDMA1X-RTT, GPRS, or another. The Access-Request might involve other messages such as PAP/CHAP or another form of authentication.

The **Flow 1c** Access-Request might contain a prepaid specific VSA, CRB_AUTH_REASON. Table 6-2 lists the attributes included in the authentication Access-Request. This tells the Cisco AR 3.5 server to authenticate the subscriber with the Prepaid server as well. If the value is CRB_AR_INIT_AUTHENTICATE, the initial quota must be obtained for a single service prepaid solution. If this VSA is not present, the Cisco AR 3.5 server will not authenticate with the Prepaid billing server.

Table 6-2 Attributes Sent During Subscriber Authentication

Attribute Number	Attribute Name	Description	Notes
1	User-Name	APPL: Mobile Node Username	Required
2	NAS IP Address	Accounting Node IP Address	APPL: Required, POA
31	Calling-station-ID	APPL:MSISDN or IMSI	APPL: Conditional
26, 9	CRB_AUTH_REASON CRB_AR_INIT_AUTHENTICATE	Refer to VSA section	Required
26, 9	CRB_USER_ID	APPL:PDSN address or SSG address	APPL: Required, Address of the PDSN
26, 9	CRB_SERVICE_ID	APPL: Service ID such as Simple IP service, Mobile IP service, or VPN service	
26, 9	CRB_SESSION_ID	This VSA contains the session key ID information	Required; the session ID must be globally unique across all clients and across reboots of the client

In **Flow 1s**, the Cisco AR 3.5 server sends a call to the billing server to authenticate the prepaid user and possibly determine more information about the subscriber’s account. The Cisco AR 3.5 server can be configured to generate this packet flow, using a subscriber profile parameter, if the request is from a prepaid subscriber.

Access-Accept (Authentication)

Flow 2b shows the billing server returning the authentication result. The billing server returns a failure if the prepaid subscriber has an inadequate balance.

Flow 2s shows the Cisco AR 3.5 server sending the Access-Accept to the AAA client. This message flow contains at least one prepaid billing-specific VSA (listed in Table 6-3) and may contain other access technology-specific attributes.

Table 6-3 Attributes Sent to AAA client in Access-Accept (Authentication)

Attribute Number	Attribute Name	Description	Notes
26, 9	CRB__USER_TYPE CRB_AR_INIT_AUTHENTICATE	Refer to Vendor-Specific Attributes, page 6-10	Optional

Access-Request (Authorization)

In **Flow 3c**, the AAA client sends another Access-Request, this time to authorize the subscriber. Table 6-4 lists the attributes required by the Cisco AR 3.5 server to authorize the subscriber. The session key ID used must be specified using a prepaid VSA pointing to the RADIUS attribute (standard or VSA).

Table 6-4 Attributes Sent During Subscriber Authorization

Attribute Number	Attribute Name	Description	Notes
1	User-Name	APPL: Mobile Node Username	Required
2	NAS IP Address	Accounting Node IP Address	APPL: Required, POA
31	Calling-station-ID	APPL:MSISDN or IMSI	APPL: Conditional
26, 9	CRB_AUTH_REASON CRB_AR_INIT_AUTHORIZE	Refer to Vendor-Specific Attributes, page 6-10	Required
26, 9	CRB_USER_ID	APPL:PDSN address or SSG address	APPL: Required, Address of the PDSN
26, 9	CRB_SERVICE_ID	APPL: Service ID such as Simple IP service, Mobile IP service, or VPN service	
26, 9	CRB_SESSION_ID	This VSA contains the session key ID information	Required; the session ID must be globally unique across all clients and across reboots of the client

.In **Flow 3s**, the Cisco AR 3.5 server sends the Prepaid billing server to obtain a quota. The quota might contain several values depending on the number of measurement parameters chosen.

Access-Accept (Authorization)

Flow 4b shows the billing server returning the quota array for the subscriber.

In **Flow 4s**, the Cisco AR 3.5 server converts the quota array received into VSAs and sends an Access-Accept with the assembled VSAs to the AAA client. Table 6-5 lists the prepaid-specific VSAs that might be included in the Access-Accept response message sent to the AAA client. For more detailed information about the VSAs, refer to Vendor-Specific Attributes, page 6-10.

Table 6-5 Attributes Sent to AAA client in Access-Accept (Authorization)

Attribute Number	Attribute Name
26, 9	CRB_DURATION
26, 9	CRB_TOTAL_VOLUME
26, 9	CRB_UPLINK_VOLUME
26, 9	CRB_DOWNLINK_VOLUME
26, 9	CRB_TOTAL_PACKETS
26, 9	CRB_UPLINK_PACKETS
26, 9	CRB_DOWNLINK_PACKETS

Flows 3c through **4s** are repeated for every service started or restarted by the AAA client.

However, if the return parameters indicate that the authorization is rejected, an Access-Accept message is generated and sent to the client as shown in Table 6-6. When this type of error condition occurs, no other VSA is included in the Access-Accept message.

Table 6-6 Attribute Sent to Report Error Condition to AAA client

Attribute Number	Attribute Name	Description	Notes
26, 9	CRB_TERMINATE_CAUSE	Identifies why a subscriber failed authentication: 1. Exceeded the balance 2. Exceeded the overdraft 3. Bad credit 4. Services suspended 5. Invalid User	Conditional; rejection might be returned with Access-Accept and zero (0) quota

Accounting Start

In **Flow 5c**, the AAA client sends the Accounting Start. In **Flow 6s**, the Cisco AR 3.5 server replies with the Accounting-Response.

Data Flow

At this point, the data transfer begins. The AAA client monitors the subscriber's allocated quotas for metering parameters. A subscriber's Reauthorization request is generated when a quota for at least one of the metering parameters, is depleted.

Access-Request (Quota Depleted)

Flow 7c shows the client sending an Access-Request to the Cisco AR 3.5 server because at least one quota has been depleted. The Access-Request includes different measurements of how much of the quotas were used in VSA format. This enables the billing server to account for the usage and manage the subscriber's balance before assigning a new quota. Table 6-7 lists the attributes returned to the Cisco AR 3.5 server:

Table 6-7 Attributes Sent by NAS When Quota Depleted

Attribute Number	Attribute Name	Description	Notes
1	User-Name	APPL: Mobile Node Username	Conditional
2	NAS IP Address	Accounting Node IP Address	APPL: Required, POA address, or Home Node address
31	Calling-station-ID	APPL:MSISDN or IMSI	APPL: Conditional
26, 9	CRB_AUTH_REASON	Refer to VSA	Required
26, 9	CRB_USER_ID	APPL: PDSN address or SSG address	APPL: Required, address of SGSN
26, 9	CRB_DURATION	Refer to Vendor-Specific Attributes, page 6-10	Required
26, 9	CRB_TOTAL_VOLUME		Conditional
26, 9	CRB_UPLINK_VOLUME		
26, 9	CRB_DOWNLINK_VOLUME		
26, 9	CRB_TOTAL_PACKETS		
26, 9	CRB_UPLINK_PACKETS		
26, 9	CRB_DOWNLINK_PACKETS		

Accept-Accept (Quota Depleted)

Flow 7s shows the Cisco AR 3.5 server returning the used quota array to the billing server. The call includes **aaa_ebs_reauthoriz().** The billing server sends an updated quota array for the next period to the Cisco AR 3.5 server.

In **Flow 8s**, the Cisco AR 3.5 server converts the quota array into VSAs and sends them to the AAA client.

Table 6-8 Attributes Sent to AAA Client in Access-Accept (Reauthorization)

Attribute Number	Attribute Name
26, 9	CRB_USER_TYPE
26, 9	CRB_DURATION
26, 9	CRB_TOTAL_VOLUME
26, 9	CRB_UPLINK_VOLUME

Table 6-8 Attributes Sent to AAA Client in Access-Accept (Reauthorization) (continued) (continued)

Attribute Number	Attribute Name
26, 9	CRB_DOWNLINK_VOLUME
26, 9	CRB_TOTAL_PACKETS
26, 9	CRB_UPLINK_PACKETS
26, 9	CRB_DOWNLINK_PACKETS

Accounting Stop (Session End)

In **Flow 9c**, the client sends an Accounting-Stop to the Cisco AR 3.5 server to end the session. The Accounting-Stop message includes an updated quota array with the usage adjustments since the previous authorization in the VSA form.

Table 6-9 lists the attributes included in the Accounting-Stop message set to the Cisco AR 3.5 server and forwarded to the billing server.

Accounting Response (Final Status)

In **Flow 9s**, the Cisco AR 3.5 server sends the used quota array to the billing server in an Accounting-Stop message. Any values returned by the billing server in **Flow 10b** are discarded.

Flow 10s shows the Cisco AR 3.5 server sending final Accounting-Response message to the AAA client.

Table 6-9 Attributes Sent in Accounting-Stop Message

Attribute Number	Attribute Name	Description	Notes
1	User-Name	APPL: Mobile Node Username	Conditional
2	NAS IP Address	Accounting Node IP Address	APPL: Required, POA
31	Calling-station-ID	APPL:MSISDN or IMSI	APPL: Conditional
40, 2	Acct_status_type	Indicates the accounting “Stop” for the service	Required; this value (2) indicates an Accounting-Stop request message
42	Acct-Input-Octets	The number of octets sent by the subscriber; uplink	Required
43	Acc_Output_Octets	The number of octets received by the subscriber; downlink	
46	Acct-Session-Time	Duration of the session	
47	Acct-Input-Packets	Number of packets sent by the subscriber	
48	Acct-Output-Packets	Number of packets received by the subscriber	
49	Acct-Terminate-Cause	This parameter, used for tracking, should remain the same for all accounting requests for a given service.	

Table 6-9 Attributes Sent in Accounting-Stop Message (continued)

Attribute Number	Attribute Name	Description	Notes
26, 9	CRB_DURATION	Refer to Vendor-Specific Attributes, page 6-10	Conditional
26, 9	CRB_TOTAL_VOLUME		
26, 9	CRB_UPLINK_VOLUME		
26, 9	CRB_DOWNLINK_VOLUME		
26, 9	CRB_TOTAL_PACKETS		
26, 9	CRB_UPLINK_PACKETS		
26, 9	CRB_DOWNLINK_PACKETS		
26, 9	CRB_SESSION_ID	Specifies the RADIUS attribute carrying the session ID information	Optional

Vendor-Specific Attributes

Vendor-specific attributes are included in specific RADIUS packets to communicate prepaid user balance information from the Cisco AR 3.5 server to the AAA client, and actual usage, either interim or total, between the NAS and the Cisco AR 3.5 Server.

Table 6-10 lists the VSAs that will be defined in the API. Table 6-10 also lists the string to be used with Cisco-AVPair below the VSA.

Note Notice that all VSAs start with CRB which stands for Cisco Radius Billing.

Table 6-10 Vendor-Specific Attributes for the Cisco Prepaid Billing Solution

VSA Name	Type	Source (Call Flow)	Description
CRB_AUTH_REASON crb-auth-reason	Int8	1c, 7c, 7’c	Passed with re-authorization: 1. Quota depleted 2. QOS changed 3. Initial Authentication 4. Initial Authorization
CRB_USER_ID crb-user-id	String	1c, 7c, 7’c	APPL: In PDSN this can be Address of the PDSN.
CRB_SERVICE_ID crb-service-id	String	1c, 7c	Identifies the subscriber’s service

Table 6-10 Vendor-Specific Attributes for the Cisco Prepaid Billing Solution

VSA Name	Type	Source (Call Flow)	Description
CRB_USER_TYPE crb-entity-type	Int8	4s	Type of user: 1. Prepaid user 2. Post-paid with no credit limit 3. Post-paid with credit limit 4. Invalid user The source for this VSA value could be from the Subscriber profile or from the billing server
CRB_DURATION crb-duration	Int32	4s, 8s	Downlink quota received by the AAA client
CRB_TOTAL_VOLUME crb-total-volume			Total Volume quota received by the AAA client
CRB_UPLINK_VOLUME crb-uplink-volume			Uplink volume quota received by the AAA client
CRB_DOWNLINK_VOLUME crb-downlink-volume			Uplink Volume quota received by the AAA client
CRB_TOTAL_PACKETS crb-total-packets			Downlink Packet quota received by the AAA client
CRB_UPLINK_PACKETS crb-uplink-packets			Uplink Packet quota received by the AAA client
CRB_DOWNLINK_PACKETS crb-downlink-packets			Uplink Volume quota received by the AAA client
CRB_SESSION_ID crb-session-id	String		Additional field if session ID is required. This VSA provides the real time billing-specific session ID. This VSA duplicates the contents of the technology-specific session ID or the contents of RADIUS attributes 44 or 50. The NAS can use this VSA to generate a unique session ID. If this VSA is not present, then RADIUS attribute 44 is used instead. If this is a string AV Pair-type attribute, the name is the string attribute name.

Table 6-10 Vendor-Specific Attributes for the Cisco Prepaid Billing Solution

VSA Name	Type	Source (Call Flow)	Description
CRB_TERMINATE_CAUSE crb-terminate-cause	Int8	4se	Identifies why a subscriber failed authentication: 1. Exceeded the balance 2. Exceeded the overdraft 3. Bad credit 4. Services suspended 5. Invalid User
CRB_PRIVATE crb-private	String	n/a	Reserved for future use

GLOSSARY

A

Access point A device that bridges the wireless link on one side to the wired network on the other.

Analog Channel A circuit-switched communication path intended to carry 3.1 KHz audio in each direction.

ARP Address Resolution Protocol is the TCP/IP protocol that translates an Internet address into the hardware address of a network interface card.

ATM Asynchronous Transfer Mode is a virtual circuit, fast packet technology. Traffic of all kinds (data, voice, video) is divided into 53-byte cells and conducted over very high speed media.

ATO Adaptive Time Out is the time that must elapse before an acknowledgment is considered lost. After a time out, the sliding window is partially closed and the ATO is backed off.

C

Call A connection or attempted connection between two terminal end points on a PSTN or ISDN; for example, a telephone call between two modems.

CHAP Challenge Authentication Protocol is a PPP cryptographic challenge/response authentication protocol in which the clear text password is not passed in the clear over the line.

CLID Calling Line ID indicates to the receiver of a call, the phone number of the caller.

CM Cable Modem is usually a modem with an RF (cable) interface on one side and an Ethernet interface on the other. A cable modem might also have a telephone interface for “telco return,” which is used when only downstream capability exists in the cable plant.

CNR Cisco Network Registrar—A network management application which includes a DHCP server and a DNS server.

Community String A string used to authenticate the trap message sender (SNMP agent) to the trap recipient (SNMP management station).

Control Messages Control messages are exchanged between LAC, LNS pairs, and operate in-band within the tunnel protocol. Control messages govern aspects of the tunnel and sessions within the tunnel.

CSG Cable Systems Group is a billing systems company.

CSR Customer Service Representative—the person you call to activate or obtain service for your account.

C

CSU/DSU Channel Service Unit/Data Service Unit isolates your network from your exchange carrier's network. It also receives the timing, low-level framing information, and data passed from the termination point. CSU/DSUs are specific to the general circuit type.

Customer A user of an ISP or an enterprise. The provider offers the customer MPLS VPN service. The enterprise provides the customer remote user access to various sites. In the case of ISPs, MPLS BPN provides a scalable wholesale access/open access solution.

D

DAP Directory Access Protocol is a heavyweight protocol that runs over a full OSI stack and requires a significant amount of computing resources to run.

Data Source Sets of data and their associated environments which include operating system, DBMS, and network platforms used to access the DBMS that an application wants to access.

DHCP Dynamic Host Configuration Protocol—a protocol that describes the service of providing and managing IP addresses to clients on a network.

DHCP Client The IOS DHCP client used to generate requests for host addresses and subnets for non-PPP clients.

DHCP Proxy Client The IOS DHCP client used to request an address for a PPP user from a DHCP server.

Dial Use Dial Use is an end-system or router attached to an on-demand PSTN or ISDN, which is either the initiator or recipient of a call.

Digital Channel Digital Channel is a circuit-switched communication path that is intended to carry digital information in each direction.

DNIS Dialed Number Information String is an indication to the receiver of a call as to what phone number the caller used to reach it.

Driver Manager A special library that manages communication between applications and drivers. Applications call ODBC API functions in the driver managers which load and call one or more drivers on behalf of the applications.

E

EAP Extensible Authentication Protocol is a framework for a family of PPP authentication protocols, including cleartext, challenge/response, and arbitrary dialog sequences.

F

FT Field Technician is someone who installs your cable modem in your house.

Frame Relay Frame Relay is a cost-effective, lightweight, many-to-many, medium-speed, virtual network, link-layer technology.

I

ISDN Integrated Services Digital Network enables synchronous PPP access.

ISP Internet Service Provider is a company that provides Internet connectivity.

H

HDLC High-level Data Link Control is both a point-to-point and multiparty link-layer technology. HDLC provides reliable, acknowledged transfer across dedicated links.

L

L2TP Access Concentrator (LAC) LAC is a device attached to one or more PSTN or ISDN lines capable of PPP operation and of handling the L2TP protocol. The LAC needs only to implement the media over which L2TP is to operate to pass traffic to one or more LNSs. It may tunnel any protocol carried within PPP.

LAN Local Area Network consists of all of the components that create a system up to a router. These components include cables, repeaters, bridges, and software up to the network layer.

LDAP Lightweight Directory Access Protocol provides a standard way for Internet clients, applications, and WWW servers to access directory information across the Internet such as user names, e-mail addresses, security certificates, and other contact information.

LEAP Light Extensible Authentication Protocol—

LLC Logical Link Control is an interface that defines several common interfaces between higher-level protocols (for example, IP) and the networks they ride upon (for example, Ethernet, Token Ring, and others).

L2TP Network Server (LNS) An LNS operates on any platform capable of PPP termination. The LNS handles the server side of the L2TP protocol. Since L2TP relies only on the single media over which L2TP tunnels arrive, the LNS may have only a single LAN or WAN interface, yet still be able to terminate calls arriving at any LAC's full range of PPP interfaces (async, synchronous ISDN, V.120, etc.).

M

MIB Management Information Base—Database of network management information used and maintained by a network management protocol such as SNMP. The value of a MIB object can be changed or retrieved using SNMP commands. MIB objects are organized in a tree structure that includes public and private branches.

MPLS Multi-Protocol Label Switching—

MPLS VPN MPLS-based Virtual Private Networks

MSO Multiple System Operators are typically cable companies that provide Internet access for regional independent operators.

N

NAS Network Access Server is a device providing temporary, on-demand network access to users. This access is point-to-point using PSTN or ISDN lines. A NAS operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers.

In PPTP terminology, this is referred to as the PPTP Access Concentrator (PAC). In L2TP terminology, the NAS is referred to as the L2TP Access Concentrator (LAC).

NCP Network Control Protocol is responsible for negotiating the protocol-specific particulars of the point-to-point protocol (PPP) link.

Network Access Identifier In order to provide for the routing of RADIUS authentication and accounting requests, the UserID field used in PPP and in the subsequent RADIUS authentication and accounting requests, known as the Network Access Identifier (NAI), may contain structure. This structure provides a means by which the RADIUS proxy locates the RADIUS server that is to receive the request. This same structure may also be used to locate the tunnel end point when domain-based tunneling is used.

O

ODBC Open Database Connectivity—a standard set of application programming interface (API) function calls (supported by Microsoft and in general use) that can be used to access data store in both relational and non-relational database management systems (DBMSs).

ODBC Driver Processes ODBC function calls, submits SQL requests to specific data source, and returns results to applications. ODBC drivers for specific types of data files, including database files, spreadsheet files, and text fields, are available from Microsoft Corporation.

P

packet A block of data in a standard format for transmission.

PAP Password Authentication Protocol is a simple PPP authentication mechanism in which a cleartext username and password are transmitted to prove identity.

Payload The contents of a request packet.

PDU Protocol Data Unit—An SNMP compliant request, response, or trap message.

PE Router Provider Edge router—a router located at the edge of the provider's MPLS core network.

POP Point of Presence is the dial-in point or connection point for users connecting to an ISP.

PPD Packet Processing Delay is the amount of time required for each peer to process the maximum amount of data buffered in their offered receive packet window. The PPD is the value exchanged between the LAC and LNS when a call is established. For the LNS, this number should be small. For an LAC supporting modem connections, this number could be significant.

PPP Point-to-Point Protocol—a multiprotocol and includes UDP, Frame Relay PVC, and X.25 VC.

Profile A collection of one or more attributes that describe how a user should be configured; for example, a profile may contain an attribute whose value specifies the type of connection service to provide the user, such as PPP, SLIP, or Telnet. Profiles can be set up for a specific user or can be shared amongst users.

Provider Service Provider—A provider who operates the access networks and MPLS backbone and provides MPLS VPN service on the backbone.

PSTN Public Switched Telephone Network enables async PPP through modems.

Q

Quality of Service (QOS) A given Quality of Service level is sometimes required for a given user being tunneled between an LNS-LAC pair. For this scenario, a unique L2TP tunnel is created (generally on top of a new SVC) and encapsulated directly on top of the media providing the indicated QOS.

R

RAC Client The IOS DHCP client used to generate requests for host addresses and subnets for non-PPP clients.

RADIUS Remote Authentication Dial-In User Service. The RADIUS protocol provides a method that allows multiple dial-in Network Access Server (NAS) devices to share a common authentication database.

RADIUS Client A Network Access Server (NAS) operates as a client of RADIUS. The client is responsible for passing user information to designated RADIUS servers, and then acting on the response that is returned. A RADIUS server can act as a proxy client to other RADIUS servers.

R

RADIUS Dictionary The RADIUS dictionary passes information between a script and the RADIUS server, or between scripts running on a single packet.

RADIUS Proxy In order to provide for the routing of RADIUS authentication and accounting requests, a RADIUS proxy may be employed. To the NAS, the RADIUS proxy appears to act as a RADIUS server, whereas to the RADIUS server the proxy appears to act as a RADIUS client.

RADIUS Server A server that is responsible for receiving user connection requests, authenticating the user, and then returning all of the configuration information necessary for the client to deliver the service to the user.

RAS Remote Access Services. See RADIUS Client.

Remote DHCP Server Usually a DHCP server in the service provider's networks, however it might also be a DHCP server in the customer's VPN.

Remote Server A server that has been registered with the user interface, which can later be referenced as a proxy client or as the method to perform a service; for example, a remote RADIUS server can be specified to act as a proxy client.

REX RADIUS EXtension allows you to write C and C++ programs to affect the behavior of Cisco Access Registrar.

Roaming The ability to connect to a NAS that is not your normal POP (Point of Presence) and have the Access-Request redirected to your normal RADIUS server. The ability to use any one of multiple Internet server providers, while maintaining a formal, customer-vendor relationship with only one.

Router A network device that connects multiple network segments and forwards packets from one network to another. The router must determine how to forward a packet based on addresses, network traffic, and cost.

Routing Tables A table that lists all of the possible paths data can take to get from a source to a destination. Depending on how routers are configured, they may build their tables dynamically by trading information with other routers, or they may be statically configured in advance.

RTT Round-Trip Time is the estimated round-trip time for an Acknowledgment to be received for a given transmitted packet. When the network link is a local network, this delay will be minimal (if not zero). When the network link is the Internet, this delay could be substantial and vary widely. RTT is adaptive; it adjusts to include the PPD (Packet Processing Delay) and whatever shifting network delays contribute to the time between a packet being transmitted and receiving its acknowledgment.

S

SAP Service Access Points (source and destination) identify protocols from which a packet has come and to which a packet must be delivered.

Script Instructions that are run in the context of a RADIUS client/server session. Scripts can be specified for servers, clients, vendors, and services. A script can be used as an incoming script, an outgoing script, or both. Incoming scripts are executed during the Access-Request portion of a dial-in session. Outgoing scripts are executed during the Access-Accept portion of a dial-in session. Scripts are referenced within the User Interface by name. Scripts can be source code for a scripting language or a binary file.

S

Service A means of specifying the method to use to perform a function. A service can be specified for the following functions: authentication, authorization, accounting, and authentication-authorization. For example, a service can specify that authentication be performed using the local database, or a service can specify that accounting be supported by logging information to a file.

Services Three default services are referenced by the server configuration and when processing scripts. They are Default Authentication Service, Default Authorization Service, and Default Accounting Service. Each service has a type and (if it is using remote servers) an ordered list of servers to use.

Session Each service provided by the NAS to a dial-in user constitutes a session, with the beginning of the session defined as the point where service is first provided and the end of the session defined as the point where service is ended. Depending on NAS support capabilities, a user may have multiple sessions in parallel or in series.

SHA-1 Secure Hash Algorithm; a hashing algorithm that produces a 160-bit digest based upon the input. The algorithm produces SHA passwords that are irreversible or prohibitively expensive to reverse.

Shared Secret Used to authenticate transactions between the client and the RADIUS server. The shared secret is never sent over the network.

Shared Use Network An IP dial-up network whose use is shared by two or more organizations. Shared use networks typically implement distributed authentication and accounting in order to facilitate the relationship amongst the sharing parties.

Silently Discard RADIUS discards the packet without further processing. The server logs an error, including the contents of the silently discarded packet, and records the event in a statistics counter.

SLIP Serial Line Internet Protocol is TCP/IP over direct connections and modems, which allows one computer to connect to another or to a whole network.

SMDS Switched Multi-megabit Data Service is a high-speed Metropolitan-Area Networking technology that behaves like a LAN.

SSHA Netscape’s (iPlanet) enhancement of the SHA-1 algorithm which includes *salted* password data.

SNAP SubNetwork Access Protocol is used when a SAP definition does not exist for the encapsulated user data protocol.

SSL Secure Socket Layer is the protocol defined by Netscape that is used for encryption and authentication between two Internet entities. It uses public/private key certificates instead of shared secrets.

SVC Switched Virtual Circuit is an L2TP-compatible media on top of which L2TP is directly encapsulated. SVCs are dynamically created, permitting tunnel media to be created dynamically in response to desired LNS-LAC connectivity requirements.

T

TACACS Terminal Access Controller Access Control System, a an authentication server that validates user IDs and passwords, thus controlling entry into systems.

Telnet A service that lets you log in to a system over a network just as though you were logging in from a remote character terminal attached to the system. It is commonly used to provide an Internet service that is exactly the same as the one you would get if you dialed into the system directly with a modem.

Trap A network message of a specific format issued by an SNMP entity on behalf of a network management agent application. A trap is used to provide the management station with an asynchronous notification of an event.

Tunnel A tunnel is defined by an LNS-LAC pair. The tunnel carries PPP datagrams between the LAC and the LNS; many sessions can be multiplexed over a single tunnel. A control connection operating in band over the same tunnel controls the establishment, release, and maintenance of sessions and of the tunnel itself.

Tunnel Network Server A server that terminates a tunnel. In PPTP terminology, this is known as the PPTP Network Server (PNS). In L2TP terminology, this is known as the L2TP Network Server (LNS).

U

UDP User Datagram Protocol, a data packet protocol.

User List The list of users registered for dial-in access.

User Record The UserRecord contains all the information that needs to be accessed at runtime about a particular user. This enables it to be read in one database operation in order to minimize the cost of authenticating the user. The UserRecord is stored as an encrypted string in the MCD database, because it contains the user’s password, amongst other things.

Users Users are represented by entities in specific UserLists. See User Record.

V

Vendor Each NAS has a vendor associated with it. A vendor may specify attributes for the NAS that are not part of the standard specification.

VHG Virtual Home Gateway—a Cisco IOS component that terminates PPP sessions. It is owned and managed by the service provider on behalf of its customer to provide access to remote users of that customer’s network. a single service provider device (router) may host multiple VHGs of different customers. a VHG may be dynamically brought up and down based on the access pattern of the remote users. Note that there is no single IOS feature called the VHG; it is a collection of function and features (PPP, virtual profiles, VRFs, etc.).

V

VPN Virtual Private Network is a way for companies to use the Internet to securely transport private data.

VRF Virtual routing and forwarding. A per VPM routing table on the PE router. Each VPN instantiated on that PE router has its own VRF.

X

X.25 A reliable public data network technology consisting of private virtual circuits, virtual calling, and per-packet charging.

X.500 Defines the Directory Access Protocol (DAP) for clients to use when contacting directory servers. DAP is a heavyweight protocol that runs over a full OSI stack and requires a significant amount of computing resources to run.

INDEX